VIRTUAL SPACE

GUARANTEES OF JURISDICTION IN THE RESILIENCE AND IN THE DEFENSE OF NATIONAL SECURITY

ROME - Farnesina Palace
11-12 October 2024

Conference proceedings

Quaderno della Rivista Trimestrale
della Scuola di Perfezionamento per le Forze di Polizia

I 2025

The seminar was organised together with the Presidency of the Council of Ministers, the Ministries of Foreign Affairs and International Cooperation, the Interior and the Justice, the National Cybersecurity Agency and the Department of Information for Security.

We thank Acea, Agenzia dell'Entrate, Camera di Commercio, Coldiretti, and Osservatorio Agromafie for their valuable contribution.

Special thanks go to

Dr. Andrea Apollonio,
Deputy Prosecutor at the Court of Patti,

Dr. Andrea Daranghi of Agenzia
dell'Entrate,

Dr. Carola Desideri
of Acea,

Dr. Tiziana Leone
of the Presidency of the Council of Ministers,

Dr. Simona Ragazzi,
GIP at the Court of Catania,

and the Vittorio Occorsio Foundation team, coordinated by Dr. Jasmin Petti and composed of Dr. Joseph Omari and Dr. Filippo Iacomini.

The reception was organised by the students
of the 'Francesco Morano' High School of Caivano (NA).

TABLE OF CONTENTS

PREFACE

Maurizio Vallone
Director of the Police Force Training School

For several years now, the Police Force Training School, in collaboration with the Vittorio Occorsio Foundation, has been addressing the issues of new technological frontiers, which offer innovative opportunities to the Police Forces for a more effective fight against organised crime, international terrorism and economic crime. The same technologies, on the other hand, are now widely used by the criminal world to make communications unintercepteable, financial flows untraceable, to create new opportunities for illicit business and thus increase the ability to commit crimes and conceal profits.

The endeavour of the School and the Occorsio Foundation is to enable both the attendees of the Advanced Training Courses and the participants at the conferences, such as the one held on 11 and 12 October 2024, which is the subject of this publication, to acquire the best legal and technical knowledge of the digital world, where technology is now inseparable from investigative techniques and is indispensable for them: it can therefore no longer be confined to the knowledge and activities of specialist experts, but must constitute the common heritage of investigators and those called upon to direct investigative or investigative coordination offices.

In this context, the topic of Artificial Intelligence and its applications to the world of intelligence and crime is increasingly being addressed, a topic of close legal and operational relevance, but which should be assessed from an evolutionary and prospective perspective, avoiding 'caging it' in hasty legal definitions that technology, in the space of a few months, could easily make obsolete and no longer responding to the new technical standards.

In fact, artificial intelligence is defined by the AI Act of the European Union (Art. 3) as *'an automated (machine-based) system designed to operate with different levels of autonomy and which can show adaptive capabilities after installation and which, for explicit or implicit purposes, deduces, from the input it receives, how to generate output such as predictions, content, recommendations or decisions that can influence physical or virtual environments*'.

It is absolutely clear that the vision of the European legislator is based on the only known examples of AI to date, such as Chat GPT-type text applications.

Actually, a scientific definition of Artificial Intelligence does not exist from a computer science point of view: the term AI is simply used as a syno-

nym for software, i.e. a computer programme capable of generating output against an input. But all software programmes have always done exactly that.

Even a simple addition is nothing more than an input (add 2 + 2) whose result (output) is the generation of a new datum (the 4).

Expectations about the adaptive or generative capacity of AI also remain, at the moment, fascinating suggestions: computer programmes, even the most sophisticated ones, do only and exactly what they are asked to do and, even when they generate a product that did not exist before, they do so on the basis of a precise programme and according to the logics that are imposed on it (algorithm).

The product of software that provides an argued outcome by acquiring from the web everything it finds on the question it is asked, and which orders the outcomes of the search according to probabilistic logical sequences (if 10 sources say that Napoleon's horse was white, it is plausible that it really was, so the AI will tell me that Napoleon's horse was white) cannot be considered generative.

If this is the case, governing AI means regulating the information concretely available to the software, in order to be sure that the output product is acceptably verified.

Indeed, if the scope of the information search is that of my computer domain (my PC, my home or professional network, the set of domains whose information supply processes I know), I can be sure that the output will provide me with a 'clean' and 'verified' product.

Conversely, if the source of the information sought by the software is the web, or even the dark web, and the system is capable of detecting and systematising by itself the information fished out of unverified spheres - which is what happens today with AI software - then the output cannot be called certified, because the deductive process may be conditioned by erroneous or deliberately artefactual information on the web.

One only has to think of the smear campaigns of celebrities or politicians during election campaigns, aimed precisely at discrediting such people and influencing electoral contests.

This is all the more true when it comes to controversial topics where, precisely on the web, disinformation campaigns are unleashed by militant individuals who are very active in the IT sphere (e.g. the NO VAX or the so-called Terra-Platterists).

Ultimately, the fundamental problem related to AI is that of 'authentication of sources': of governing those sources from which software draws the information that it then analyses to produce the final product to be delivered to the user.

On the authentication of sources much is discussed and often in the end thrown in the towel, due to the extreme difficulty of envisaging, in today"s world, a system that can effectively guarantee that the final product is based only on qualified and certified sources.

Who is capable of certifying the billions of pieces of information circulating on the web? Obviously no one, not even the most powerful of machines.

And then: can we limit the development of AI? Can we require producers to certify their sources? And where can we attempt to do this? The European Union has intervened with the AI ACT. Well, can we justifiably assume that potentially hostile (or even economically competitive) countries can accept restrictions on their digital capabilities in the name of a "Cyber Democracy"?

The issue of rules in this field is a matter of great importance for the competitiveness of our companies, of our defence (General Carmine Masiello, Chief of Staff of the Army, has represented the danger that regulatory limitations on the use of artificial intelligence in Europe and in Italy could weaken our capacity for technological evolution in the fields of defence and military intelligence vis-à-vis potentially hostile foreign subjects that do not have similar limitations), the Public Administration itself, which, in order to be effective and efficient and to meet the challenges of the coming years, must necessarily avail itself of extremely high-performance AI tools capable of constituting a top-level aid to the operator as well as support to the decision-maker.

Alongside the issue of source certification, there is the inescapable importance of the ethical use of AI.

The topic is so important that the Italian G7 Presidency included it on the agenda of the summit of Heads of State and Government last June in Puglia. This session was opened, for the first time in history, testifying to the importance of the topic, by His Holiness Pope Francis, who recalled how "*it is from the use of this creative potential that God has given us that artificial intelligence comes into being. The latter, as is well known, is an extremely powerful tool, employed in so many areas of human endeavour: from medicine to the world of work, from culture to communication, from education to politics. And it is now safe to assume that its use will increasingly influence the way we live, our social relationships and in the future even the way we conceive of our identity as human beings*".

The Holy Father therefore reminds us of the need for a common ethical root in the application of any tool, be it computer or manual.

Well, the Ai Act is based on the principle that AI must be developed and used in a safe, ethical manner that respects fundamental rights and Euro-

pean values. For this reason, the regulation provides for a classification of AI systems according to their level of risk to the security and rights of individuals, and sets out a series of requirements and obligations for providers and users of such systems. Thus, AI can never be used except in accordance with our constitutional principles, and thus never for racial, sexual, religious profiling, etc., or to create discrimination or aggravate conditions of social hardship.

We come, therefore, not to a general certification of everything AI produces, but to a conscious use of that product.

We can and must use AI to speed up production processes and rationalise the certified information already in our possession, to put it at the basis of decisions that, as such, will be the result of a greater information contribution, already rationalised and organised, to allow the decision-maker a faster "precedent" and support the final decision that, if it implies third-party rights, must be taken with the full knowledge that the information on which it rests is authentic and the result of a "humanisation" that only the intellect and professionalism of a human being can operate.

Vito Tenore (President of the Chamber of the Court of Auditors) recently published an essay entitled *"Can AI replace the judge?*". Well, it will be able to do so in countries where the human component is not relevant in the decision of a dispute. Certainly, and in line with the author, it will not be able to happen in Italy where, in addition to recent regulatory provisions, primary value is given to the case-by-case assessment that only the judge can give to the outcome of the trial.

Obviously, AI can also be widely used in our judicial system, to systematise acts, to search for the maxims of the Supreme Court with greater speed and completeness, to search for similarities and precedents in the now vast field of European jurisprudence and international courts, all of which are certified acts that can be effectively summarised and brought to the attention of the judge, who will draw from them for his own determinations.

I would like to thank the Occorsio Foundation for the great and effective contribution it makes to the School in terms of training on subjects of great complexity and innovation, and in particular Prosecutor Giovanni Salvi, all the members of the Scientific Committee, and the speakers at the various conferences.

Oreste Pollicino

Full Professor of Constitutional Law at Bocconi Univeristy, Italian Representative at the European Agency for the Protection of Fundamental Rights, Special Advisor FVO

In the era of advanced digitalisation and frontier artificial intelligence, cyberspace is configured as the new theatre of global confrontation, where disinformation, cyber attacks and algorithmic manipulation threaten not only national security, but also the resilience of democratic institutions. Jurisdiction, as underlined by Giovanni Salvi in his introduction, is not only a mechanism for regulating conflicts, but an indispensable garrison of sovereignty and rule of law, called upon today to respond to challenges of unprecedented complexity.

Malicious operations in cyberspace are characterised by a combination of opacity, transnationality and volatility, elements that challenge traditional legal instruments. The difficulty of attributing responsibility, combined with the need to act quickly, calls for a rethinking of regulatory and procedural strategies. It is not only a matter of identifying the perpetrators of cybercrimes, but of preventing and mitigating damage through coordination between intelligence, jurisdiction and international cooperation.

A central theme that emerged during the conference was the regulation of disinformation as an instrument of political and social destabilisation. The manipulation of information, amplified by increasingly sophisticated artificial intelligence algorithms, represents a systemic threat. As highlighted by Salvi, disinformation does not only affect public trust, but acts directly on democratic decision-making processes, requiring multi-level regulatory intervention. It is in this context that co-regulation emerges as a particularly promising strategy, as it aims to combine the flexibility of private authority with the guarantee of public control.

In this respect, the new European regulatory season, embodied by the Digital Services Act (DSA) and the Artificial Intelligence Act (AI Act), witnesses a significant paradigm shift. Indeed, the transition from algorithmic automation to the decision-making autonomy of artificial intelligence introduces new challenges, especially with regard to the protection of fundamental rights. Whereas the regulation of automation algorithms focused mainly on system reliability and data protection, the decision-making autonomy of AI requires even stricter control to ensure that systems do not operate in a way that is detrimental to individual or collective rights.

The distinction between automation and autonomy is crucial: automation concerns mechanical or algorithmic processes that perform tasks accord-

ing to predetermined rules, while autonomy implies the ability of a system to learn, adapt and make decisions independently. This shift implies a necessary evolution of the regulatory framework towards a model that integrates principles of transparency, accountability and constant human supervision.

A further important element is the emergence of private digital powers of a quasi-sovereign nature, capable of influencing public debate and conditioning the functioning of democracies. The jurisdictional response to such powers cannot be limited to the mere enforcement of pre-existing rules, but must be proactive and creative, favouring the introduction of new enforcement tools that ensure an effective balance between innovation and the protection of rights.

In this sense, co-regulation presents itself as a particularly effective model. It involves close collaboration between public authorities and private actors, with the aim of defining common standards and ensuring compliance through shared control mechanisms. Such an approach makes it possible to overcome the rigidities of traditional regulation and to respond more quickly and appropriately to the constant changes in the technological environment.

International cooperation was a further thread running through the conference, highlighting how no country can tackle the challenges posed by cyberspace alone. Instruments such as the Second Additional Protocol to the Budapest Convention and the future UN Convention on Cybercrimes represent important steps towards a shared legal framework, but there are still many open questions. Mr. Salvi emphasised the importance of developing an international consensus based on common values and the sharing of best practices to ensure a coordinated and effective response to transnational digital threats.

Finally, the conference highlighted how the regulation of cyberspace and artificial intelligence cannot ignore a constitutional perspective. The balance between innovation and the protection of rights must be the guiding principle of any regulatory intervention. Only an integrated approach, combining security, international cooperation and the protection of fundamental rights, can guarantee institutional resilience adequate to the challenges of the future.

INTRODUCTION

Giovanni Salvi
President of the FVO Scientific Committee, Former Attorney General at the Court of Cassation

From 11 to 12 October 2024 held in the MAECI headquarters, Farnesina Palace, the seminar "*Virtual Space. The Guarantees of Jurisdiction in the resilience and in the defense of national security*", organised by the Vittorio Occorsio Foundation in collaboration with the Presidency of the Council of Ministers, within the framework of the G7 Italian Presidency.

The proceedings were introduced by Vittorio Occorsio, on behalf of the Foundation and his father Eugenio, by the Vice-President of the Scientific Stefano Lucchini and the Secretary General of the Farnesina, Ambassador Riccardo Guariglia, The Vice-President of the CSM, Fabio Pinelli, the President of the Superior School of the Judiciary, President Emeritus of the Constitutional Court, Silvana Sciarra, and the Attorney General of the Court of Appeal of Rome, Giuseppe Amato, contributed with non-formal but richly contained greetings.

The seminar was attended by Ministers Matteo Piantedosi and Carlo Nordio, Undersecretary Alfredo Mantovano - in addition to greetings from Minister Antonio Tajani - the President of COPASIR, Lorenzo Guerini, and representatives at the highest level of the Department of Information for Security (DIS) - Deputy Director Alessandra Guidi - the National Authority for Cybersecurity (ANC) - Director Bruno Frattasi and Deputy Director Nunzia Ciardi -, the Court of Cassation and the General Prosecutor's Offices of Cassation and Appeal, representatives of the judiciary, European and Italian institutions, and international experts.

The opening day was introduced by the report of Prof. Paola Severino and technical reports by Dr. Keiko Kono and Lt. Col. Massimiliano Signoretti.

Work continued in the three sessions on specific topics, chaired by Prefect Alessandro Pansa, the Secretary General of the Court of Cassation, Stefano Mogini, and the Attorney General of the Court of Cassation., Luigi Salvato

The potential applications of the new cooperation measures and the complex relationship between jurisdiction and intelligence were discussed by experts in public international law. These included the Vice President of the

International Criminal Court Judge Rosario Aitala, Prof. Marko Milanovic, currently responsible for the drafting of the Tallinn 3 Manual of the *NATO Centre of Excellence* (CCDCOE)- Lt. Col. Massimiliano Signoretti, former Italian expert in the drafting of the Tallinn Manual 2, Danilo Ceccarelli, representative of the European Public Prosecutor's Office, Judge Antonio Balsamo, international expert and former President of the Court of Palermo, Professors Oreste Pollicino and Marco Roscini, among the leading experts in international law, Ambassador Denis Craig Wilder.

Representatives from Italy (Minister Plenipotentiary Michele Giacomelli and Head of Department of the Ministry of Justice Luigi Birritteri) and other countries and supranational institutions (UN Secretary-General's High Envoy for Technology, Amandeep Singh Gill, UNODC representative Glen Prichard, US Ambassador Deborah Mc Carthy and the representative of the Brazilian Ministry of Foreign Affairs, Eric Do Val Lacerda Sogocio, both vice-chairs of the *Ad Hoc Committee on Cybercrime Convention*) presented the status of the work of *the UN Open Ended Working Group on Security of and in the use of Information and Communication Technologies* (OEWG) on Virtual Space and the outline of the Cybercrime Convention, finally approved by the Committee.

Finally, experts from various judicial and bodies law enforcement (Postal and Telecommunications Police, Eurojust and Europol) discussed the implications of new technologies on investigative tools, in particular with reference to crypto-platforms; coordinated by magistrate Eugenio Albamonte, Ivano Gabrielli, discussed the topic Hannes Glantshnig and Edvardas Sileris .

In the news section of the site, you can see the full programme and a link to the live streams Youtube of the two-day conference:

https://www.fondazioneoccorsio.it/virtual-space/

The Seminar is also the fruit of cooperation with the Interior Ministry's Interforce School. The joint work has led to the inclusion in the School's programmes of the Vittorio Occorsio Courses, intended for high-level officers and officials, also from other countries, who participate each year in the structured training offered by the School. The courses explore, also in workshop mode and with the contribution of experiences of different origins, the investigation and procedural tools required to deal with the new technologies.

Similar courses are organised every year at the Superior School of the Judiciary.

The Seminar is part of this path and we are therefore very pleased and honoured to be able to publish the proceedings in the *Quaderno della Rivista Trimestrale della Scuola di Perfezionamento per le Forze di Polizia*, which

has already seen other contributions from the Foundation. The publication is also in English, so that it can be fully utilised by all those attending the School. It may form the basis for further reflections and for the liaison work between the Academy, the Police Force and the Judiciary, which is the primary objective of the Foundation.

The seminar focuses on how to make the exercise of jurisdiction effective for the most serious transnational crimes committed in whole or in part in Virtual Space, and how to relate jurisdiction to the exercise of other sovereign powers that in turn are undergoing processes of transformation with respect to challenging technological transitions.

Transnationality is intrinsic to cybercrime. The most serious cybercrimes can also affect a nation's critical infrastructure. In recent years, the major infrastructures of some countries have been the target of attacks of varying nature and severity. The attacks have also affected the most sensitive decision-making processes in a democratic regime, those of consensus building in elections, and those supporting the decisions of public bodies.

The growing capabilities of offensive tools that rely on Frontier AI to evolve autonomously make these attacks increasingly effective and countermeasures increasingly difficult.

In the past year, the Japanese-led G7 produced two important results concerning *Frontier AI* and the need for a global approach to these challenges (*Hiroshima Process on AI*). The Italian-led G7 intended to continue along this path.

Without an understanding of these dynamics, it is futile to address the issues of defence against cyberattacks and its implications on the dislocation of powers and guarantees.

For this reason, the seminar opens with a review of the most recent and significant findings by researchers who participated in the drafting of those conclusions.

Malicious operations carried out with advanced cyber tools actually affect several aspects of national sovereignty at the same time. A cyberattack targeting critical facilities constitutes first and foremost a crime, according to the expectations of most countries. The UN Convention on Cybercrime, which is in the process of being approved by the UN General Assembly, provides for the necessary punishment of the most serious conduct and aims to universalise the principles of the Budapest Convention, which has already been signed by 75 countries.

Such operations require at the same time a reaction from the attacked state aimed at reducing the damage and preventing future damage.

Finally, attacks constitute a violation of sovereignty and - in the most

serious cases - legitimise forms of reaction that can go as far as a kinetic response against the state to which the action is attributed.

The three levels of significance of the malicious operation interfere with each other and therefore require serious coordination, first and foremost at national level.

The most recent legislative interventions in Italy have primarily extended the powers of action aimed at resilience (attributed to the National Counter-Terrorism Authority) and active prevention, as well as offensive response, attributed to the intelligence services; the possibility of resorting to infiltration and undercover operations has also been strengthened, with the aim of obtaining useful elements to establish responsibility, but also to interrupt the ongoing conduct and *to disrupt* the hostile IT tool.

Among the problems that such novelties pose is the relationship between the three levels of reaction, so that they do not interfere with each other and end up hindering each other.

Central, from the point of view of jurisdiction, is now the role played by the National Anti-Mafia and Terrorism Prosecutor's Office, a body entrusted with the role of coordinating these relations, while the judicial authority and the NCA are charged with the task of safeguarding the different needs of the two distinct and sometimes conflicting approaches. Suffice it to think of the issue of the integrity of evidence for criminal purposes, which is called into question by immediate defensive interventions that are manipulative in themselves.

The potential interferences are very wide-ranging. One in particular deserves specific attention: the effectiveness of ex post forms of intelligence, police and judicial cooperation.

Jurisdiction is faced with the difficulty arising from the transnationality of operations, which are further characterised - in the specific case we are dealing with - by volatility, opacity, non-localisation, non-deterministic logic and therefore difficult to reconstruct the path of the algorithms a posteriori. All this implies that international collaboration mechanisms based on the subsequent consent of states to the acquisition of evidence are de facto ineffective, at least in some of the modes of attack.

Difficulties in gathering evidence are common to different legal systems. The United States has had, for many years now, a regulatory instrument to overcome some of these difficulties: the Cloud Act. It attempts to overcome the difficult obstacle constituted by the real dislocation of powers in the SV, between national states, supranational institutions and large private groups.

Despite significant achievements, even the US has recognised the diffi-

culty of effectively exercising criminal jurisdiction in the SV. Recently, *the Deputy Attorney General* with delegated authority for this area, Lisa Monaco, clearly stated that *"rather than focusing on arrests, US law enforcement is trying to prevent additional victims of the crimes"* (24 April 2023). The consequence is that *"to combat cybercrime, US LE increasingly prioritises disruption"*.

The pliability of the US legal system allows this prospective limitation, although some have commented that in the past this would have been considered heresy (*"In days gone by, that might have been heresy"*). There is no doubt, however, that it ends up assimilating the criminal trial, by its very nature aimed at ascertaining personal responsibility for acts provided for by law as crimes, to the other forms of legitimate exercise of sovereign powers.

In our legal system, however, such a programmatic limitation would not be acceptable.

The nation states face a not dissimilar problem, due to the specific characteristics in which it takes place in the IS.

The legitimate exercise of reaction powers, including those that are limited to the violation of the sovereignty of other nations, not to mention offensive cyber or kinetic responses, must in fact come to terms with the institution of *attribution*, i.e. the international community's agreement that the malicious operation originated from one or more states; either as direct attackers or as non-compliant with due diligence obligations.

The challenge is not an *actio finium regundorum* between different powers of the state for supremacy purposes. On the contrary, safeguarding the effectiveness of jurisdiction in the SVC is an absolute necessity in order to ensure the transparency of operations - to the extent possible and without prejudice to the competing and legitimate powers of other powers of the State - and respect for the *Rule of Law*.

Intelligence bodies are also, in our legal system, subject to the law and form part of the rule of law. These very characteristics, however, allow for covert action, protected by secrecy.

Thus, jurisdiction is also a measure to protect the international community against the risk of escalation, which is inextricably linked to the use of covert means of penetration and reaction. This is all the more relevant considering the intertwining of malicious operations and conflict, whether fought or creeping.

The potential of future hybrid warfare is enormous, partly still unexplored. What seemed a long way off yesterday is now a reality. Conflicts, in particular the Ukrainian one, demonstrate the offensive potential, still partly held back by the awareness of the global risks that can arise from the use of

ICT in covert forms. The use of *Autonomous Lethal Weapons*(ALW), drones capable of operating en masse, of augmented reality capable of assessing the situation on the ground, has established itself as an ordinary reality of the new conflicts3.

The implications are enormous and not yet fully analysed. The competitive advantage of ALWs is all the greater the less functioning the mechanisms of authorisation by the human being are. The paradigm of the *Human in the Loop*, or even in *Command,* risks remaining an ethical prescription, soon to be clouded by the need for the instrument to be able to compete with similar, but unconstrained, nations that do not wish to submit to that precept. In normative, not just ethical terms, these precepts are affirmed as obligations to insert *by default* restrictive mechanisms (authorisation, consent, control, etc.), as envisaged in general by the *EU IA Act* (in the absence of supranational regulation of ALWs). However, not all states adhere to this approach and thus gain an enormous competitive advantage over slower and less precise apparatuses because they require human control.

But that is not all. The application - of which we know nothing for obvious reasons of secrecy - of ever more advanced and complex logics may lead to the autonomy of the Frontier AI apparatus, as defined, for example, in the UK *Frontier AI*, which has been mentioned and is the subject of analysis in the seminar.

The challenge is therefore very complex. It ends up affecting international cooperation mechanisms themselves, rendering obsolete those based on subsequent consent - destined to be totally ineffective in transnational cyber operations - and consequently having to focus on cooperation instruments structured in advance and thus based on the prior consent of states to interference in their sphere of sovereignty. This is the direction in which both the Budapest Convention and its Second Additional Protocol and the draft UN Convention on Cybercrime are heading.

But these measures do not allow effective action to be taken against malicious acts, in particular those that constitute a crime, by individuals and states that do not submit to the provisions of the conventions, to which, moreover, a minority of states are currently party.

This raises the serious problem of domestic law and international law as to what actions are legitimate to react to such attacks. Firstly, the issue of the attribution, for the purposes of recognition by the international community, of the legitimacy of the attacked state's reactions. Secondly, of the modalities and limits (of legitimacy and effectiveness) of the instrument of criminal law, once the epitome of national sovereignty.

These themes can be summarised in four areas, which were the subject

of the seminar, which also saw them developed in the lively debate between the speakers and the audience:

a) Limits of multilevel international cooperation resulting from the specific characteristics of the FVC;
b) Instruments to make this cooperation effective (stabilisation of the Joint Investigation Corps and provision for subsequent validation);
c) Actions that nation states may legitimately take under public international law to defend themselves against attacks from non-cooperating countries; conditions and limits;
d) Legal instruments currently available in Italy (Intelligence and Law Enforcement) to act in cases sub c).

Finally, the public debate itself on these issues can be undermined by malicious actions in cyberspace. Disinformation mechanisms affect trust in public space, undermining one of the essential components of democracy. The line from the Marx Brothers becomes prophetic: "who do you believe, me or your own eyes!".

Jurisdiction is not the solution but only a part of it. A part that is perhaps minor but of considerable relevance. The aim of the seminar, made evident by the unravelling of the interventions in the four sessions, is to identify what are the spaces for the effectiveness - and not just the prescription - of jurisdiction, in relation to the exercise of other powers, a legitimate and increasingly intrusive manifestation of sovereignty.

OPENING SESSION

PRESENTATION OF THE FVO AND MEMORY OF VITTORIO OCCORSIO

Vittorio Occorsio
Co-founder FVO

On behalf of the Vittorio Occorsio Foundation and my father Eugenio, I welcome you to this important conference dedicated to two topics of extraordinary topicality and relevance: Jurisdiction in Virtual Space and the role of Artificial Intelligence in legal dynamics.

The digital era has radically transformed the way we live, interact and do business. In particular, the internet and the most advanced technologies have broken down physical and geographical boundaries, opening up completely new and complex legal scenarios.

The very notion of space, which will be the subject of the conference, has undergone an epochal change. Today, the concept of physical space coexists with that of virtual space, an environment in which individuals, companies and governments operate through digital networks, often without regard to territoriality. However, this transformation poses crucial challenges to law, which is traditionally based on national borders and jurisdictional norms anchored in the physicality of states. In this context, one of the main questions is how we can define and regulate jurisdiction in a space that has no tangible borders.

There, I could go on with this tenor, except that when I was preparing my speech in the previous days, I did an experiment and I asked Chat GPT to generate an introductory paper for a conference on Virtual Space. Chat GPT generated for me the two paragraphs, I just read there. It became apparent to me that I needed to change my approach.

The profession of conference introducer is, in fact, one of the closest to disappearance.

Since the technical interventions will be many and more qualified than mine, I prefer to talk about something Chat GPT cannot replicate: feelings. And there are two feelings with which I participate in this introduction to the proceedings. The first, I must say, is a feeling of sadness and emptiness. Obviously, I would not be here if my grandfather, a magistrate, had not been killed in 1976 here in Rome by a fascist terrorist group, a victim, like so many

others, in the years of lead, in that season that bloodied the country from 1969 to 1984. An innocent victim, but an aware one. Occorsio had grasped a series of correlations between the organised underworld, including the Mafia, and then the Roman underworld that would generate the Banda della Magliana, some extreme right-wing subversive organisations, and finally some international and national occult organisations. A few days before he was killed, he had launched an investigation into the relations between kidnappings, organised crime and a Masonic Lodge, which would later turn out to be Licio Gelli's Propaganda 2 Lodge. Five years before the Castiglion Fibocchi kidnapping.

His professional and human story was perhaps unique because, as prosecutor in the Piazza Fontana trial and having arrested Valpreda, he was accused by the anarchists and the left of being a conservative. Then, when he had the "Ordine Nuovo" movement declared illegal - as a reconstruction of the fascist party - the neo-fascists said he was on the other side. Swung from one side to the other, eventually he paid a heavy price

The second feeling is the opposite of the first, it is a feeling of joy and pride: the excitement of seeing the fruit of our Foundation's work. When we set it up in 2020, and remember this Giovanni Salvi and Stefano Lucchini - to whom my profound gratitude goes - we wanted to create a space of freedom, where the best energies of the country could come together, to preserve the memory of our past and, at the same time, think about our future. We do not intend to be custodians of the ashes, but we think that, in order to focus on the future, an awareness of who and how it was that allowed us to live in this country, with these values, is essential. We cannot take anything for granted, as evidenced by the wars, discrimination, violence, and the new technocratic imperialism we are witnessing.

A space of freedom, because all the people who generously lend their time for the Foundation know that there are no pre-established ideological structures and that confrontation and respect for the ideas of others is the essence of our values. Freedom, of course, is not anarchy; on the contrary, awareness of deep ethical values, not flaunted in a sometimes trivialising manner. Respect for others, which is the counterpart of freedom, respect for working people, and there have been many here for this conference. First of all, I would like to thank Professor Melina Decaro, Secretary General of the Foundation and to whom we owe not only the commitment of organisational coordination but also the contribution of reflection on the constitutional implications of the topics we are addressing today. I would also like to thank Tiziana, Jasmin, Carola, Andrea, Joseph, Filippo, all the people in our Foundation who worked, and the other organisations who collaborated. I am think-

ing, for example, of Coldiretti, Osservatorio Agromafie, Professor Eugenia Carfora, headmistress of the Caivano High School. Here you have seen the boys from the I.S. "F. Morano", with whom our Foundation has been working for some time, in uniform, and we are happy to have them here today, even in this different context.

In all those who generously participate in the life of the Foundation, I have seen profound ideals and values, from which satisfaction and hope derive, in the mindful memory of a season where those ideals and values led to the violent deaths of many. Yesterday, for example, was the anniversary of Girolamo Tartaglione, another magistrate killed in Rome two years after Vittorio Occorsio, this time by the Brigate Rosse.

The faces of the victims of the years of lead, of terrorism, of so many Magistrates, functionary of Arma dei Carabinieri, Guardia di Finanza, Police, who fought to give us the free way of life we know today, we see them again in their colleagues, in their students. It is a joy to see that the Foundation is a home for magistrates and law enforcement officers, committed to working for the future, always keeping their memory of the past.

At the conference that opens, the defence of the Republic, the defence of nation states, will be discussed. Here, defence moves to other planes, that of advanced technology, but it always requires - I borrow an expression dear to Giovanni Salvi - *the ancient virtue of courage*, from the days of the defence of the Republic of Athens to today, to virtual space: today as yesterday, it is to the courage of us all that we must refer. Good work.

PRESENTATION OF THE SEMINAR

Stefano Lucchini
Vice President FVO Scientific Committee - Chief Institutional Affairs and External Communication Officer of Intesa Sanpaolo

Hello everyone and welcome, I am Stefano Lucchini.

Thank you, Vittorio. I can only be happy and thank all the participants in the meantime and add something personal. I can only attribute and be grateful to Giovanni Salvi, who was the animator, as well as to Vittorio and Eugenio Occorsio for the passion that the Foundation manages to involve.

I join in thanking Professor Carfora and my friends at Coldiretti. I thank the Foreign Ministry for this hospitality and the team for the organisation.

I would like to try to articulate this short introductory speech of mine in three parts.

In the first part I would like to discuss the technological, social and ethical-constitutional transformations taking place, starting with the theme that brings us together today in this beautiful setting.

I would like, in particular, to start with the first two words in the title that has been given to this very important occasion for study and reflection: "virtual space". I interpret this as an almost provocative reference to what, in the past - because it is always important to learn lessons from the past - has been considered the main characteristic of cyberspace: a space, that of the world of bits, precisely, of a virtual nature, almost in opposition to the real space proper to the world of atoms.

Let us take a step back a few years, so as to fully grasp those lessons of the past to which I referred, and avoid, today as we set out to regulate the complex axis of the digital ecosystem constituted by Artificial Intelligence, making the same mistakes or, simply, naivety.

These errors characterised the original debate on web regulation. Davos, 1997, World Economic Forum: *Governments of the world, weary giants of flesh and steel, I come from cyberspace, new abode of the mind. On behalf of the future, I ask you, beings of the past, to leave us alone. You are not welcome among us. You have no sovereignty over the places where we meet*.

Of course, these are provocations. If there were still any doubts about how the network order was conceived by the founding fathers of the early period of the web, this passage from Barlow's might be useful in dispelling them. It is an order, or rather a new imagined virtual order, characterised by

an absolute discontinuity with respect to the state order, not only because of the detachment and spatio-temporal separation from the latter, but also because of the revolutionary value attributed to the network community, capable of regulating itself without any filter of institutions, public powers and social formations of an intermediate nature, characterised by that *Declaration of Independence of Cyberspace* structural of the legal order understood in the Roman sense.

Almost thirty years later, it is easy to conclude that history has brought out a very different reality from the one Barlow hoped for. Perhaps better, for at least two reasons.

The first is that nation-states have shown that they can not only regulate, but also hyper-regulate cyberspace, which it is always good to keep in mind: even before bits, it is made up of physical infrastructures, submarine cables and therefore an atomic dimension, part of that analogue world against which Barlow proclaimed himself a rebel. States, today, have shown themselves capable of creating great virtual walls, as in the case of the Chinese Great Firewall and, most recently, the Russian one, following the invasion of Ukraine, which sees virtual walls and strategies that should have been, according to the utopian vision of the pioneers of the new digital frontier, a new world free from conditioning and strong powers, in which the continuity of users would have had the capacity to self-regulate themselves in the light of a reference value framework founded on the freedom of the network and in the network, turned out to be a space that, far from wanting to straddle the equally harmful visions of the utopian and dystopian ones, e.g. of Morozov and partially of other personalities, turned out to be very accessible to private powers that have certainly conditioned that process of self-determination on the part of users, which was supposed to be the cornerstone on which to build the space imagined by the web pioneers.

This is, in my opinion, the conceptual humus within which the very stimulating and complementary perspectives that characterise these two days of work can be framed. We are very curious to understand and see what will then emerge in a synthesis from these two very important days. Instead, the second part of this speech aims to focus on identifying a few basic questions that seem to me to characterise a common denominator, a red thread, of these themes that will be authoritatively developed during these two days. It is often said that the real difficulty in constructing a path of innovative investigation does not lie in giving the right answers, but in formulating the most appropriate questions to open such a path.

And so we asked ourselves a few questions, without ambitions of exclusivity. It might perhaps be useful for the work of these two days to investigate

what are the reasons for the ongoing transfiguration of the major technology platforms from mere economic actors to real private powers, often in competition with public ones. Is the transformation of the European regulatory instrument proportional and adequate to cope with this transfiguration? And again, what are the new challenges posed by the emergence of generative Artificial Intelligence? Why does it require a regulatory reaction, but also a constitutional framework of containment different from those that characterised the reaction to the emergence of the algorithmic factor? And what, finally, is the difference in terms of the constitutional principles at stake between the automation underlying the season of the algorithm and autonomy, spatio-temporal acceleration, inference and predictivity, which, on the other hand, constitute the essential characteristics of the new digital ecosystem constituted by this Artificial Intelligence that has been so bursting at the seams in recent years?

I leave it to you to try and give some initial answers to these questions, assuming you find them interesting, of course. And finally, the last part of this brief introduction, in the light of the reflections I tried to develop at the beginning. It is clear that the issues under investigation and reflection today are anything but virtual. National security, sovereignty, territory are categories of constitutional law that are still, as current events confirm, alive and well even in cyberspace and have a real, tangible impact on the daily lives of us all.

Let me focus on the issue of protecting national security, a privileged subject.

As noted recently in a fine article in Il Sole 24 Ore by Prefect Frattasi and Professor Pollicino, over the last few years cybersecurity and related issues, treated in an increasingly systemic manner, have raised concerns about the resilience of, among other things, the rule of law. They have progressively placed themselves at the centre of general attention, going well beyond the niche dimension for specialists that characterised their early beginnings, both in terms of the interest of the doctrine, especially with regard to institutional implications, and of jurisprudence.

In this context, cybersecurity is increasingly emerging as a fundamental right of the individual, endowed with its own axiological and conceptual autonomy. There is still no recognition of the right to cybersecurity as an autonomous substantive position of the individual. However, a change of approach is already present also in the national context, in view of the widening of the number of subjects to whom the relevant cybersecurity rules are addressed, whose full implementation reverberates in the protection of citizens from the threat to their freedom in the digital dimension, following also in this latter dimension a prismatic conception of security, long highlighted in the public debate.

I am drawing to a conclusion. In my opinion, a compass for today's work, and more generally for the great challenges of this acceleration of change, could be precisely to look at security as a right to freedom, as, moreover, constitutionally enshrined in Article 5 of the Charter of Fundamental Rights of the European Union, where it expressly states that everyone has the right to freedom and security. It codifies that conceptual combination of freedom and security that it would be very dangerous to split.

INSTITUTIONAL GREETINGS

Riccardo Guariglia
Secretary General of the Ministry of Foreign Affairs and International Cooperation

I am Riccardo Guariglia, Secretary General of the Ministry of Foreign Affairs, and also on behalf of Minister Tajani I would like to welcome you to the Farnesina. As you know, the Farnesina is the home of Italian diplomacy, a home with doors that are always open, especially for international initiatives that pertain to the vital interests of our country. In this regard, I must say that our collaboration with the Occorsio Foundation is a source of prestige for us, and so I thank you for having chosen the Farnesina, on which you can always rely, as the venue for this very important seminar.

Today's event is an initiative that we were very keen to host, precisely because of its high scientific value and the centrality of the topics chosen. I congratulate the Foundation for the very high level of speakers and guests, first and foremost, of course, the Minister who honours us with his presence here, as well as for the richness of the programme that has been outlined for today. In the context of the crises crossing today's international scenario, it would be a mistake to overlook factors such as the fifth domain, i.e. cyberspace, as well as digital transformation. Indeed, in cyberspace, geopolitical dynamics today take on a dimension that is, so to speak, more elusive than the tools of what we consider the toolbox of diplomats and all insiders. It is a domain populated by multiple actors, not always benevolent ones: I am thinking of groups conducting disinformation campaigns and attacking critical infrastructures, or of actors perpetrating various criminal activities, and I am referring not only to individuals and companies, but also to state entities. So it is a really important risk. On the other hand, technological progress has made more and more cutting-edge and sophisticated tools available to all users, which require both considerable investment and effective rules. It is precisely the new technologies that take these issues to an even more complex level. We are all fascinated by the astonishing potential of Artificial Intelligence, and the imagination runs along the plots of books and novels - there are already some dealing with this very topic - and various applications of this technology can indeed improve our lives in the fields of health, crisis and disaster prevention, public and private service delivery, and financial services, but there are many other fields that are touched upon. How much do we

really know about the risks involved? What legal implications does this impact on the world of work, on the most vulnerable groups, on international relations themselves? Our Ministry attaches particular importance to the issue of cybersecurity and new technologies, so much so that we wanted to create, under the impetus of Minister Tajani, a special unit in the secretariat general that I head. We are committed to promoting an open, free, obviously interoperable and secure cyberspace within the G7. Our commitment dates back to the Italian presidency in 2017: I remember when, on that very occasion, the Lucca Declaration of Foreign Ministers was adopted. I was there and I remember the first G7 policy document on cybersecurity, a real reference for subsequent presidencies. In keeping with this precedent, this year the Farnesina chaired the Ise-Shima Cyber Group (ISCG), which dealt with aspects of cyberdiplomacy, while the National Cybersecurity Agency convened, in May, in this very room, for the first time, the counterpart agencies of the G7 countries and the European Union.

I was keen to inaugurate both of these events because of the importance of the topic in the context of our foreign policy. Great importance was then attached to the dossiers by the Ministers of Foreign Affairs, Justice, Home Affairs, and State and Government Ministers meeting in Borgo Egnazia under the aegis of the G7 Italian Presidency. In a constantly connected world, cyberspace is increasingly contested and has become a vehicle for malicious campaigns, often linked to foreign policy objectives. This is precisely why the G7 countries expressed concern about the growing number of cyberattacks, especially ransomware, against hospitals and healthcare facilities. We reiterated our firm determination to protect our democratic systems and critical infrastructure, calling for responsible behaviour of states in cyberspace and the applicability of international law. These are, after all, the same principles for which we stand up in all multilateral fora: I am thinking of the United Nations, the European Union, NATO, the OSCE, the Council of Europe, and in the bilateral contacts we have with aligned and non-aligned countries. The aim is the implementation of specific confidence-building measures, confidence that is also needed when we look at new technologies and consider Artificial Intelligence. Trust means studying together the technical-scientific aspects of the tool and, at the same time, working out together a very important regulatory framework capable of setting ethical barriers to protect the centrality of the human being. This is the spirit that animates and has so far animated our commitment during the G7 presidency, in whose agenda, as I mentioned earlier, the President of the Council wanted to give Artificial Intelligence a real priority. The aim is to devise appropriate policies to reap the full benefits of these technologies

while mitigating the risks to society. This is the *common thread*, the *leitmotif* of our work.

To this end, the definition of an international governance of Artificial Intelligence is essential, a considerable challenge given the different approaches and sensitivities at every latitude of the globe. And on this front too, the European Union has demonstrated its ability to act as a point of reference for the entire international community, having approved in May, as you know, with the decisive contribution of our country - it is important to emphasise – the regulation, the first set of binding rules on Artificial Intelligence. In conclusion, the topics I have just mentioned and which will be at the centre of these two days of work undoubtedly deserve qualified legal insights, since much depends on cyberspace and new technologies in the development of international relations and, more generally, in the growth path of humanity. Since its beginnings, most of which took place in Rome, law has been a ductile instrument, capable of adapting to the changing socio-economic reality in order to offer effective discipline to it. It takes, of course, great commitment, great determination and, as Vittorio Occorsio said, I would stress, great courage. I absolutely agree, it is such a challenge to the ability to normalise law, which is being repeated today with the fifth domain, a fascinating challenge on which I am sure there will be authoritative interventions today and tomorrow.

Giuseppe Amato

Attorney General at the Court of Appeal - Responsible for authorising interception activities of Security Intelligence Agencies

Thank you for the welcome invitation, for which I am truly grateful. I cannot but start, as Vittorio did, with two considerations on the topics we have to talk about today. I also cannot but start with a memory, the memory of Vittorio Occorsio, whom we commemorated on 10 July this year. For me it is a special memory, because it accompanied my childhood and many personal relationships we had with grandfather Vittorio. It is a fitting remembrance and a true appreciation for what the Foundation does and will do to address important issues like the one we are dealing with today. This memory must also be a stimulus to look ahead. Precisely in connection with this need to find stimuli, today's conference is particularly significant.

Vittorio Occorsio is a victim of terrorism, and today we are talking about cybersecurity. Talking about cybersecurity also addresses the fight against attacks that may have a terrorist purpose. This makes the topic highly topical. Considering a broad notion of terrorism, certain cyberattacks fully fall into this category, given their ability to significantly interfere with the political, economic and business structures of a country. Thus, cyber security is also a fight against terrorism.

Italian public prosecutors' offices have been organised for years in the fight against cybercrime by emphasising the specialisation of magistrates. In some public prosecutors' offices, the fight against cybercrime is assigned to those who are part of counter-terrorism groups. I remember the period from 1993, with Italy's first organic law on computer crime, to the Budapest Convention and the law that implemented it. In those years we were pioneers in the fight against cybercrimes. I had the opportunity, with some colleagues, to write a book on the subject in the early 2000s. Reviewing it today, one can see how many of the fundamental arguments of the time are now outdated. At the time, we were even discussing the definition of computer documents and computer systems, whereas today we are talking about virtual spaces that still need to be filled with content, in an age of change.

Our legal system has made significant progress since then. With the establishment of the Cybersecurity Authority in 2021, an important step has been taken towards coordination between the various actors in the fight against cyber security. This coordination is not an end in itself, but must be proactive, making the most of the different resources available. Further steps were taken with the 2023 law decree, which provided for coordination for

certain crimes at the National Anti-Mafia Prosecution Office, highlighting the importance of a proactive approach, especially in a context where territoriality is increasingly marginal. Subsequently, the 2024 law strengthened both the tools available to the judiciary and the preventive ones, making all actors whose networks may be subject to attacks more responsible.

We have at our disposal an important toolkit to address the phenomenon in a meaningful way. I would like to make two reflections based on my experience as a magistrate and currently as Attorney General in Rome, with a focus on wiretapping and services. The first reflection concerns the importance of the contribution of the judiciary, not only with a view to repression, but also to prevention. Prevention is fundamental: repression is already a defeat, since it implies that the attack has already been committed. Here, a preventive approach is decisive to prevent the damage from materialising.

The second reflection concerns the activity of the Agencies and wiretapping, which are fundamental to prevent infiltration, dossier-tapping and abuse. I believe that our system is an example of a guarantee, thanks to the presence of an independent authority, compliance with the law and control by the political authorities. This system makes it possible to combine prevention and repression effectively, guaranteeing security and respect for fundamental freedoms.

I conclude by expressing confidence in the ability of our system to effectively counter these phenomena and look forward to further exploration of future prospects, also in view of the new UN convention that may bring further regulatory changes.

Fabio Pinelli
Deputy President of the Superior Council of Magistracy

The new technologies and, in particular, the application of artificial intelligence to the legal sector bring with them a series of practical consequences - still largely unforeseeable - and stimulate a reflection, both fascinating and frightening at the same time, on its repercussions in terms of the protection of fundamental rights and the role of jurisdiction.

Very appropriately, this seminar - whose title does not expressly mention artificial intelligence - has devoted its focus to the two most problematic terms that evoke it: "virtual space" and "guarantees of jurisdiction".

The new forms of crime permitted by the new technologies (on which a number of reports have focused) make it possible to raise the dangerousness of the implemented (and enforceable) conducts to the level of national security itself, thus posing a problem of reorganisation of the legal reaction, which it is important - for the very safeguard of democracy and of the legal and social conquests it has enabled - to keep within the limits of a jurisdictional response, in which criminal jurisdiction inevitably seems to play a central role: the tragic alternative would in fact be the belligerent one of the so-called cyber-wars.

However, the jurisdictional response must adapt, in order to be effective, to the characteristics of such "new conducts" and such "new forms of aggression" to fundamental legal goods, which place it in front of new and largely unprecedented limits.

The first note is that of the so-called "virtual space". In fact, the capacity for action - made possible by digitised technologies, such as those of artificial intelligence - is not only no longer limited by territorial boundaries, but no longer even presents precise physical reference points: this means, in fact, the so-called cyber-space, which in reality is a "non-space".

All this risks undermining the traditional legal instruments for determining jurisdiction by territory and the very jurisdiction of individual states, making artificial intelligence systems an elusive target that cannot be "captured" by individual legal systems.

The other side of the problem of jurisdiction and cooperation - along with the traditional guarantees that operate within them - is that of the mechanisms of imputation of responsibility (also the subject of papers in the seminar).

With respect to new artificial entities capable of autonomous choices and capable of actions that were once only possible for a human being - unimaginable just a few years ago - there is the further and serious problem of the liability of "machines" in the courts.

The dogma of *machina delinquere non potest* no longer holds water. The traditional model whereby machines are mere instruments of human criminal action is no longer applicable because the harmful result is caused by the choice of the machine alone, increasingly disconnected from the action of the man who built it and who, so to speak, has a "genetic responsibility", which is ill-suited to the traditional imputative mechanisms of malice and guilt.

There is therefore a clear risk of a vacuum of criminal protection for certain types of offence, since the imputative models of strict liability are not compatible with the principle of culpability and personality of criminal responsibility.

The individual human agents themselves, who are "genetically" responsible, are concealed and difficult to identify, since what emerges is largely only the appearance of conduct (unrelated to a human agent and referable to Bots or the like) on the various "platforms".

Here, then, is one of the most delicate issues that arise in this matter: in what terms can one speak of "platform liability"? What risks for the free manifestation of thought can lurk in the attribution of these forms of liability? What global resistance is there to this? Can they be considered surmountable?

In the face of all these difficulties, one might be tempted to say that the best answer is not the repressive-sanctuary one, but the preventive one, that is to say, that of a regulation that notes on the creation, production and use of artificial intelligence systems that act in virtual spaces.

It seems to me that this is, after all, the perspective of the European regulation adopted on 13 June 2024, containing harmonised rules on artificial intelligence.

The aim of the regulation is certainly to improve the functioning of the internal market and promote the deployment of "anthropocentric and affordable" artificial intelligence, while ensuring "a high level of protection of health, safety and fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union, including democracy, the rule of law and the protection of the environment, against harmful effects of AI systems in the Union".

However, to take as the specific object of the legislation, the circulation in the markets of artificial intelligence systems, responds to the idea that artificial intelligence systems are a "risky" product, so much so that a classification is established, which includes (in the presence of certain characteristics) the qualification in terms of a "high risk" system, and a series of guarantees and requirements are prescribed for those who produce, supply, disseminate and use them. In short - to be clearer, but trivialising a little - artificial intelli-

gence systems are like "weapons" and there must be a regulatory framework regulating their production, dissemination and use: they cannot be left entirely to individual freedom and mere market mechanisms, and perhaps not even to the isolated decisions of individual states.

In fact - and this is the other idea of great interest contained in the European legislation - the limits to the use of these new instruments (in compliance with the guarantee of fundamental rights) must also be imposed on the States and in the same criminal repression activity carried out by them: the "guaranteeist" choice is not an option that can be abandoned according to emergencies and contingencies; it must be considered an irrevocable choice, connoting every system of liberal democracy.

Such a powerful and dangerous technology for the rights of the individual, as that of artificial intelligence systems, cannot be evaluated only in terms of effectiveness and achievement of results (albeit of criminal repression), but must be surrounded by a series of guarantees and precautions peculiar to and appropriate to the risks run by its use.

Significant, in my opinion, is the fact that in implementation of these principles, the regulation deals, for example, with the use of remote "real time" biometric identification systems in publicly accessible spaces for law enforcement purposes, setting precise limits.

Thus, the needs of criminal justice do not, from the perspective of the regulation, always and in all cases permit the use of AI systems (in this case the remote biometric identification systems), but require "proportion" (necessary use), are limited only to certain "needs" and only for "serious crimes".

This seems to me to be an extremely important indication of method: the containment of the new criminality of Virtual Space through jurisdiction only makes sense insofar as it remains within the guarantees of fundamental rights that constitute it in democratic systems.

However, there do not seem to be any optimal solutions, and there is no hiding the limitations that this type of regulatory intervention entails.

First of all, there is the time lag that inevitably occurs between the timescale for adopting and implementing regulations and the development of technologies, which continue to move forward and accelerate.

In truth, Italy took immediate action and in the Council of Ministers of 23 April (about a month after the publication of the AI regulation in the EU Official Journal) a draft law on artificial intelligence was approved, which should cover five areas national strategy, national authorities, promotion actions, copyright protection and criminal sanctions; the government-initiated bill on 19 September 2024 was under consideration by the VIII and IX Joint Commissions; the document - drafted by a committee of experts to support

the government - containing the Italian Artificial Intelligence Strategy 2024-2026 has already been published.

However, a certain time lag is necessitated by implementation times, implied not only by the need to adapt national regulations, but also to respect the fundamental rights provided by the EU in favour of manufacturers and suppliers and to give them time to adapt to the new rules as well. These unavoidable needs - linked to the regulatory system and the high guarantees it provides - however, determine a time gap that, in view of the rapidity of development of these new technologies and their applications, runs the risk of legislation always lagging behind the evolution of a technology such as artificial intelligence, so much so that some have suggested using more useful and faster tools such as the adoption of technical norms and standards that, however, being rules of so-called "soft law", do not have the degree of flexibility to adapt to the new rules. soft law norms, they do not have the degree of binding force of the slower so-called hard law norms (i.e. European regulations and directives and national laws).

The lack of optimal solutions at present therefore represents a challenge that this Seminar intended to address intelligently - and with human intelligence - by taking it to the useful level, which is that of a meaningful position within the G7.

Indeed, new technologies and artificial intelligence represent an ongoing challenge to human intelligence, a challenge that is not within the reach of either individuals or individual states, but a challenge that must be addressed at a global level and that should be placed at the level of the jurisdiction, as the seat of the greatest guarantee of the fundamental rights of the individual, which are perhaps the greatest achievement of the modern legal world.

Silvana Sciarra

Former President of the Constitutional Court - President of the Superior School of the Judiciary

Thank you, thank you indeed. I am grateful to the Vittorio Occorsio Foundation for the invitation to offer my personal greetings and those of the Superior School of the Judiciary on an occasion such as today's, which is characterised by a very high level of speakers and participants and by the relevance of the topics addressed. A special greeting to the Minister. My presence confirms and is intended to confirm a now mature collaboration between the Superior School of the Judiciary and the Foundation, a fruitful collaboration that we hope will continue with even greater emphasis on these issues. This event is, among other things, a collateral event to the G7 Italian presidency, which, among other things, launched the work of the *Venice Justice Group*, which we are all already looking to in the coming weeks for further impetus to be given to the fight against organised crime in all its forms and declinations, as well as to a balanced use of Artificial Intelligence to protect democratic systems. It has been recalled, and I want to reiterate it, of the rule of law, hence of the judiciary, from that framework of reference that I believe is an indispensable framework for a full and conscious transposition of the European regulation, also just recalled, which entered into force last June, establishing harmonised rules on Artificial Intelligence, an inspiration for the activities of the Superior School of the Judiciary, in the wake, moreover, of a programme of courses that has long been underway on these and other related topics, for example on the defence of national security and the reflection on the Budapest Convention on Cyber Crime.

It is not superfluous to recall that this regulation, which was aptly mentioned by Ambassador Guariglia, aims at a better functioning of the internal market in the free movement of goods and services. Because the internal market, Europeans must be reminded, is in fact a common good which, ever since the Coal and Steel Community, has seen the founding states held together by the foundation of a single market. And then in this market there have always been other states included, so an ever-widening market. And I like to remember this because free movement, it has been said, is an exercise of freedom, and security is also an exercise of freedom. But let us remember that in the days of the Coal and Steel Community, freedom of movement was guaranteed for Italian miners who often went to work with dedication in Belgium and Germany. Today, the rules of the market must, instead, apply to Artificial Intelligence in compliance with transparent principles that must never be separated from respect for fundamental principles and rights. Recital number one

of the regulation refers to the Charter of Fundamental Rights of the European Union, a text that we must never forget, a text that, among other things, on the reminder of Recital number one, protects health and safety as primary goods, but also the rule of law and the environment. I am a great believer in these integration processes through law. Older jurists, among whom I place myself, I must say fortunately, because ages must be lived for what they are, will remember the work of a great Italian jurist, Mauro Cappelletti, who studied integration through law and went beyond Italian borders. Here, I believe that in this integration through law, in which, I repeat, I believe very much, the role of education is crucial. It was already so at the dawn of the European Economic Community, because education, precisely, was the vehicle for the full exercise of the freedoms guaranteed by the Treaties. And integration into the European Union is parallel and I would say, perhaps functional, to the better coordination of state measures in the context of the Council of Europe. Therefore, integration must be interpreted, and we have been doing so for some time, as a multi-level integration, especially to guarantee Cyber Security. The Superior School of the Judiciary invests incessantly, I would like to say, with a truly capillary activity, energies and skills in the training of Italian magistrates and, at the same time, contributes to orienting training activities in other countries. It is not only the highly respected commitment, I must say, of the School in the European network of magistrates' training schools, but also the work of dissemination of training contents and techniques that the Superior School of the Judiciary carries out in other countries. I particularly emphasise the engagement with African countries, to which we will also have the opportunity to speak, true Ambassador Guariglia, to further improve our cooperation. And with a country afflicted by an atrocious war conflict, Ukraine, which has received training from the Italian School and which is obviously interested in strengthening national security. Therefore, I believe that the complexity of the confrontation that is required today, which certainly goes beyond the sources of the European Union, makes it necessary to broaden the scope of our reflections, since it is now quite clear that Artificial Intelligence is developing on intrinsically interdisciplinary ground due to its many ethical and philosophical implications, but also due to the increasingly marked contribution of neuroscience and, if necessary, linguistics. Because Artificial Intelligence feeds on concepts and words. We all know, precisely because there are so many books, it was mentioned a moment ago, that the world of algorithms is a diverse world, even in its application to judicial systems. The implications that we understand most, because they are perhaps even closer to widespread practice, are the implications that impart efficiency to offices, creation of databases, sophisticated filing methods. All this is talked

about in school courses, but on the other hand we have to face the challenges of learning algorithms to transform inaction into experience and, what is most important, into knowledge. There is no fear, at least I have been reassured on this front, listening to the reassurances of the physical and mathematical sciences, there is no fear of replicating the human mind. But perhaps this is not enough to give impetus to an axiology of Artificial Intelligence applied to judicial systems, especially when dealing with issues related to the prevention of crimes of international relevance that arise and develop in virtual space. My personal commitment and that of the Steering Committee of the Superior School of the Judiciary is to strengthen the investment in the training of magistrates, all Italian and non-Italian magistrates, because many non-Italians pass through our classrooms, with an increasing emphasis on interdisciplinary openings to understand the use of Artificial Intelligence and its implications. We aim to do this in an even more fruitful and fruitful, if possible, collaboration with the Vittorio Occorsio Foundation. The culture of magistrates must expand in listening to other voices, it must increasingly - it already is - open up to contemporaneity in a non-acritical manner and, therefore, draw on knowledge and respect for pluralism. Knowledge of law is interwoven with data, not only drawn from material life, but also those that now float in virtual space. I also recall the close cooperation with the Interforce School here in Rome. The two schools have signed an agreement. I would also like, and this I hope is not an eclectic reference, but I do so for the benefit of the foreign guests speaking at this conference as well, to point out that in Italy there are many occasions, and not just now, already for years, so a long time ago, of confrontation between secular and religious thought on the issues of Artificial Intelligence and its applications to jurisdiction. One may recall the experience of the so-called Courtyard of the Gentiles, which is a high-level occasion of confrontation between the secular and the religious, which among other things promotes debates and publications of great interest on our themes. But let me mention a recent book that has a catchy title: *The Algorithm of Life*, which has as its subtitle *Ethics and Artificial Intelligence*, written by Vincenzo Paglia, president of the Pontifical Academy for Life is fuelling reflections on the ethical implications of Artificial Intelligence programmes. On the other hand, it was precisely in Rome in 2020 that the *Rome Call for AI Ethics* took place, which is certainly inspired by the social values of the Church, but promotes an interdisciplinary monitoring of technologies and even a transdisciplinary ethics. Thus it does not fail to emphasise the legal sphere because it affirms the protection of persons. The author of this book begins with a quotation from Genesis, which, as a lay person, I repropose to emphasise work as a common commitment. In the hope that these reminders do not sound, as I

said before, perhaps a little extraneous, even eclectic compared to the other themes of this conference, but this is a high reminder, because in the Garden of Eden man was placed to cultivate and guard it, and today we look at the work of magistrates and those who work alongside them in combating and preventing international crimes, as a work that is about to move into virtual space without ever losing its anchorage to fundamental values, those that are precisely planted in this garden to be guarded and cultivated.

OPENING OF THE WORKS

Carlo Nordio
Minister of Justice

Thank you for the invitation. Host, Ambassador Guariglia, President, dear colleague Giuseppe Amato, gentlemen of the authorities. First of course, or as they say last but not least, Vittorio Occorsio. I too would like to start this short speech with a memory: when Vittorio Occorsio was killed, I was taking the oral exams to enter the judiciary in Rome. This shows both my age and the emotion with which I recall that episode. The president of the commission at the time, a great jurist, his name was Mario, commented that we would not make it to Christmas, since they had killed three in three days. I say this because the tribute paid by the judiciary, to which I still belong, in the fight against terrorism, and which has in Vittorio Occorsio one of its most eminent and significant figures, is a tribute that honours the order to which I belonged and to which, I repeat, I still belong, albeit as a minister.

As far as today's speech is concerned, which as you can see is done at arm's length, the technical aspects will be much more authoritatively dealt with than the scarce knowledge, so to speak "cybernetic", of myself, the staff and the members of our Ministry. I will limit myself to a few general remarks.

The first concerns the relationship between law and technology. Man, in his characteristic free spirit, has the capacity for invention. As far as the production of law is concerned, we many times find ourselves in what the philosopher called the paradox of Achilles and the tortoise: as Achilles tries to reach the tortoise, the tortoise steps forward and Achilles will never reach it. Why do I say this? Because when there is a technological innovation, the law is very often lacking, and the legislator is forced to chase the problems that emerge from the technological innovation. This is even dangerous in the penal system, because of the gaps in protection that exist."

We all know that the criminal law is not retroactive and therefore it is not possible to incriminate a certain behaviour if it was not previously provided for by law. This requires us to work imaginatively to understand what problems technological innovation poses. This has always been the case, even in civil law. Just think of the problems that have arisen with artificial insemination, with the new boundaries and concepts of death and life.

It was once thought that life was born with lung docimasia, today we know that the irreversible identification of a person's genetic code occurs

much earlier. It was once thought that death coincided with the stopping of the heartbeat, today we know that it is the flat electroencephalogram that gives us this knowledge, and that therefore one can even proceed with a stopped heart. So much so that transplants are done. You all remember how difficult it was, and still is today, to regulate these technological innovations, especially in the field of end-of-life care, precisely because technology confronts us with problems that were once unthinkable.

So it is with cyber security, so it is with Artificial Intelligence. Technological innovation, telematics, digitisation, right up to the creation of this sort of *monstrum*, which is not at all, of Artificial Intelligence, has created and continues to create problems. But the message with which I want to begin, and shortly conclude, this speech is that we must convert these possible criticalities into opportunities.

Technological tools are never good or bad, they are neutral. Atomic fission is also neutral: it can create great energy, but it can also create Hiroshima. Nuclear fusion is even more important: if we succeeded with nuclear fusion in transforming a bottle of water into energy, we could light up the entire city of Rome for 50 years. If instead we misuse it, we have a bomb explosion. It was called Tsar, and in 1961 it had the power of 50 megatons, or 50 million tons of TNT, enough to destroy the entire region of Lazio.

And so it is with Artificial Intelligence, and so with all technology. If we know how to use it well, we will have a great opportunity; if we use it badly, we will have devastating problems.

The presence of large criminal organisations in what until yesterday was only a communication system, and which today is instead a tool for creating ideas, presents us with new challenges. But even here we must be careful not to confuse Artificial Intelligence with the human brain.

I privately attended the presentation of the book mentioned by President Sciarra, written by Monsignor Paglia, on the algorithm of life, and I am honoured by the friendship of Cardinal Ravasi, who established the Cortile dei Gentili, also mentioned above. Human intelligence, the ability to distinguish not only the logical from the illogical, but also the good from the bad, is a deep-rooted theme in our culture. It is written in the Bible. President Sciarra mentioned the Garden of Eden. If we read Genesis, we see that when Adam eats the forbidden fruit, God says: "Behold, he has become like one of us, for he knows the difference between good and evil."

Eating the forbidden fruit is a mythological representation of the evolution of human intelligence. This evolution has distinguished man from animal, because before, not knowing how to distinguish good from evil, man - or rather, that creature that was perhaps not even man - was akin to an animal, a

vegetable. If you do not know how to distinguish good from evil, you cannot choose either one or the other and you are deprived of moral autonomy. You are not a moral being, but an undifferentiated being. And there intelligence was born, there morality, ethics were born.

We are inclusive monopolists of this intelligence. There is no possibility of an Artificial Intelligence replacing or substituting itself for human intelligence. Artificial Intelligence is a product of man, as are algorithms and, in the future, so will be algorithms of algorithms. They will be able to replicate, but not create; that would be a fictitious creation.

I believe that with Artificial Intelligence one could, for example, reconstruct a Bach suite with new chords, maintaining the same relationships between the harmonies of the various sections and sequences. Artificial Intelligence could create a seventh suite for solo cello, but it would not be a Bach suite. It would be a replica, similar to what *madonnari* make on the floors of the Duomo: copies of Michelangelo, but not Michelangelo himself. They are simply a *copy and paste* with a different size to the original.

From human intelligence and the freedoms of the spirit comes the conclusion I would like to reach: we must not be afraid of the new cyber-innovation and, in particular, Artificial Intelligence. They are our creatures, which must be managed by the human brain and, above all, the human heart.

The first to invent a kind of Artificial Intelligence, a small electronic brain, i.e. a small calculator, was none other than a great philosopher: Blaise Pascal. He built the first calculator, which is still called the "pascaline". This same philosopher and scientist wrote one of the most beautiful thoughts in the history of philosophy: the human being is endowed with an *esprit de géométrie* and an *esprit de finesse*. The *esprit de géométrie* concerns the brain, logic; the *esprit de finesse* concerns the heart, ethics.

If we manage to combine both these possibilities, as Pascal wanted, then Artificial Intelligence will not be a danger, but a great opportunity.

Giovanni Salvi

President of the FVO Scientific Committee, Former Attorney General at the Court of Cassation

My speech is an out-of-plan, which I hope will be useful to introduce our next two speakers who will talk to us about the more advanced aspects of Artificial Intelligence, which emerged in the course of the Japanese-led G7 and then in the work of the Group *UK Frontier AI*, so that from this approach we can then draw, in subsequent work, the consequences for our specific field of work. The focus of our work, actually, in the mare magnum of issues that arise in cyber, is on a very specific topic, which has already been introduced by Minister Nordio and Attorney General Amato: the role of jurisdiction in this new challenge and its relationship with other forms of sovereign powers.

Jurisdiction is not merely asserted, because any state can assert its universal jurisdiction; making it effective is quite another matter, especially in a situation where other actors are also involved. It is true that jurisdiction is fundamental, and we will see this in the development of all this work, but making it effective also means relating to other actors, who are now the ones who actually operate effectively in this sector: from resilience, in our case the National Cyber Security Authority, to the Intelligence sector, which is now of very great importance.

We should have had the National Anti-Mafia Prosecutor, Giovanni Melillo, here today. Unfortunately, for serious and personal reasons, in the past few days he has had to withdraw, and so this absence has meant that the introduction to the many problems faced in the relationship between resilience, intelligence and jurisdiction, also as a result of the recent regulatory changes in Italy and the many supranational regulatory interventions, either in place or under discussion, has been lacking. And so I try, immodestly, to give some indication on some of these aspects, to explain the sense of the succession of reports in the seminar. Then we have here the Deputy National Prosecutor, Michele Prestipino, who, if he would like to speak at the end of the presentations, will give us a great gift.

Thus, transnationality inherent in cybercrime. The most serious cybercrimes can affect a nation's critical facilities. In recent years, the major infrastructures of some countries have been the target of attacks of various kinds, and none of them can be considered safe. For instance, the most frequent and most serious attacks have occurred against healthcare, one of the most critical infrastructures for national security.

The increasing capabilities of offensive tools that rely on frontier Arti-

ficial Intelligence to evolve autonomously make these attacks increasingly effective and countermeasures increasingly difficult.

The Japanese-led G7 has produced two important outcomes in the past year about the impending challenges of AI and the need for a global approach to these challenges. The *Hiroshima Process on AI,* addresses the issues of defence against cyberattacks and its implications on the dislocation of powers and safeguards. Dr Keiko Kono, who took part in the process, will talk to us about this process.

The approach aimed at regulation on the part of the international community was then developed in the work of the Group organised by the United Kingdom, which produced, at the end of 2023, an important elaboration, again within the G7 framework, condensed in the document *UK AI Frontier*, which analyses the current state of "frontier" Artificial Intelligence, its unforeseen speed of development and new perspectives, for the coming years.

The ethical, framework regulatory and technical that emerges from all these initiatives is indispensable to put the discussion on the effectiveness of jurisdiction in the Virtual Space on a basis of reality, eschewing easy prescriptive approaches: for instance, the *Human in the Loop* is certainly an ethical imperative and can be transfused into norms, but how to make them effectively binding in transnationality?

For these reasons, the seminar opens with a review of these acquisitions by researchers who participated in that work. We should have had the deputy director of the British Institute; she too, unfortunately, has had serious health reasons in the past few days, for which we wish her well, and so she will not be there, but she is worthily replaced by Lieutenant Colonel Massimiliano Signoretti, who has long dealt with these matters.

Malicious operations carried out with advanced cyber tools are in fact simultaneously relevant to several aspects of national sovereignty. A cyberattack targeting critical facilities is first and foremost a crime, according to most countries, and the UN Convention on Cybercrime, the final text of which will be under discussion in the General Assembly in the coming months, will provide a further catalogue of these crimes, which will then become recognised in forms shared by most countries in the world.

Such operations require at the same time a reaction from the attacked state aimed at reducing the damage and preventing future damage, which is the typical attribution of resilience structures, such as our NCA.

Finally, attacks constitute a violation of sovereignty and, in the most serious cases, legitimise forms of reaction that can go as far as a kinetic response against the state to which the action is attributed.

The three levels of malicious operation interfere with each other and

therefore require serious coordination, first and foremost at national level. Recent legislative interventions in Italy have extended the powers of actions aimed at resilience and active prevention, as well as offensive response. This, attributed to the Intelligence Agencies, has been strengthened. The possibility of resorting to operations undercover, of infiltration into the attacking information structures, is then attributed both to the police, with the authorisation of the judicial authority, and to the Intelligence.

Among the problems posed by these novelties is therefore the relationship between the three levels of reaction, to ensure that they do not interfere with each other and end up hindering each other. Central from the point of view of jurisdiction is the role now played by the National Anti-Mafia and Anti-Terrorism Prosecution Office. However, the potential for interference is very broad. In fact, some of the major operations that have enabled the eradication of criminal structures such as crypto platforms are the result not of decryption of algorithms, but of combined operations in which intelligence played a significant, perhaps central role. Thus, what appeared to us to be an operation to break the encryption of algorithms, in reality often had a traditional intelligence and penetration operation behind it.

Consequently, the collection of evidence for use in criminal proceedings does not only encounter the issue of the back-readability of the algorithm. The issue also becomes that of evidence from intelligence. Depending on the trial systems, this evidence may or may not be admissible, and in any case follows differentiated procedures. This is an additional issue to the one traditionally addressed in courtrooms of the transparency of decryption operations.

The jurisdiction faces the difficulty arising from the transnationality of transactions, further characterised in our specific case by volatility, opacity, non-localisation and non-deterministic logic.

This implies that international cooperation mechanisms, based on the subsequent consent of states to the acquisition of evidence, are de facto ineffective. Soon the new fundamental European provisions on electronic evidence gathering will come into force. But the difficulties in gathering evidence are common to the different legal systems. The United States, which has been working on this for many years, has long since put in place a regulatory instrument to overcome some of these difficulties: the *Cloud Act*. It attempts to overcome the difficult obstacle constituted by the real dislocation of powers in virtual space between nation states, supranational institutions and large private groups.

The large private groups operate in Virtual Space as a sort of new East India Company, exercising de facto regulatory and authoritative powers that

were once the prerogative of the nation state, indeed the privileged terrain in which its essential characteristic, sovereignty, was manifested. If partnership is now indispensable, this does not detract from the fact that the exercise of jurisdiction, at least by its intrinsic characteristics in the rule of law, cannot be conditioned by the consent of those who actually exercise those powers.

Even the amendment of *Rule 41* of the *Federal Rules of Criminal Procedure* in the United States did not solve this problem for activities that take place abroad, but exclusively at home, trying to prevent additional victims of crimes. The powers of Law Enforcement, however, even after that amendment, remain confined to the domestic jurisdiction, allowing the fragmentation between the federal states to be overcome.

The consequence is that the goal of the Department of Justice, according to the indications coming from *Deputy Attorney General* Lisa Monaco, who is in charge of the matter, is to combat cybercrime by increasing the priority of *disruption*, no longer that of convicting those abroad who carry out these activities, which is in fact considered impracticable. This approach, made possible by the ductility of the US legal system, would not be imaginable in our legal system, because it would radically transform the criminal justice system.

In our legal system, this activity is attributed to intelligence. Judicial activity is secondary and as a result, because in attempting to identify and bring to punishment those responsible, we also have the opportunity to play these preventive roles.

In conclusion, all this brings us to the similarities and differences between the activities of intelligence and those of jurisdiction. This is what will be explained to us by those who, knowing these new mechanisms, can illustrate why it is extremely difficult to follow, in supranational space and in several countries, the traces of an aggression, while ensuring that the evidence is in forms that can be legitimately used in a criminal trial. Problems, these, similar to those encountered in public international law with regard to the principle of attribution, These are the serious issues that we would like to address, not to say resolve, in the development of these two days of work. Starting from the awareness that this challenge is different from those faced in the past: reaching the evidence, gathering the evidence and making it, above all, usable in the criminal trial, therefore in an adversarial process between the parties, in which secrecy either cannot enter, or enters in such a way as to guarantee the rights of the parties in any case. Making these mechanisms work implies a clear regulation of the relations between Intelligence, resilience and jurisdiction, and the ability to understand that jurisdiction beyond a certain point will not be able to reach, and that the Intelligence must, in any

case, respect the fundamental principles of the rule of law, as is already the case in our legal system.

With this introduction, I hope I have given a sense of what we are going to hear next, which will be an illustration of what is new in the field of frontier artificial intelligence. Many thanks.

INTRODUCTORY REPORT ON THE NEW FRONTIERS OF AI (STARTING WITH THE PROCESS G7 - HIROSHIMA AI PROCESS) AND THEIR EFFECTS ON NATIONAL SOVEREIGNTY AND THE EFFECTIVENESS OF THE EXERCISE OF JURISDICTION

Keiko Kono
Hiroshima AI Process Expert

It is a great honour to introduce the G7 Hiroshima AI Process today. With the advent of generative AI, criminal actors no longer need as many technical experts as before to carry out cyberattacks. Anyone can write sophisticated phishing emails, create malware and deepfake content using generative AI technology. So the efficiency of their work is dramatically improved thanks to AI technology. As a result, defending against such AI-enabled cybercrime and information operations is becoming even more challenging in terms of speed and scale. The G7 Hiroshima AI Process was launched last year with the aim of promoting the safety, security and trustworthiness of advanced AI systems, and contributing to reducing these risks. I hope that the achievements of the Hiroshima AI Process that I will present today will be relevant and contribute to the discussion at this conference. I begin the presentation with the timeline of the Hiroshima Process. Then, I briefly introduce the main document of achievements of the Hiroshima AI Process, namely the Hiroshima Process International Code of Conduct for Advanced AI Developers, including its monitoring mechanism. Finally, I conclude with some outstanding issues that lie ahead with the goal of developing an AI governance framework at the global level. During the G7 meetings in 2022, artificial intelligence was not particularly on the agenda. However, in 2023, it suddenly became one of the main topics for digital and technology ministers' meetings following the release of GPT-4 in March 2023. In May 2023, G7 leaders announced the launch of the Hiroshima AI Process to discuss common policy priorities related to generative AI. The following month, the G7 Working Group (WG) began its work at the initiative of the Japanese government, which circulated a questionnaire to G7 members to take stock of the opportunities and challenges of generative AI technologies. Considering the results of the questionnaire, they drafted outcome documents in collaboration with external experts, including the OECD. The drafting work was completed around October 9, and two documents were released by the G7 leaders at the end of the same month. One is the International Guiding Principles and the

other is the International Code of Conduct. Both documents are intended to apply to organizations developing advanced AI. On December 1, G7 digital and technology ministers agreed on the "Hiroshima AI Process Comprehensive Framework," after incorporating feedback from a stakeholder survey in the EU, Japan, and the US. The comprehensive policy framework was endorsed in a leaders' statement five days later. In 2024, AI governance remains on the agenda of G7 meetings under the Italian presidency.

In May, at an OECD event, then-Japanese Prime Minister Kishida announced the creation of the Hiroshima Process Friends Group with the participation of non-G7 countries. Currently, 53 countries and the European Union are on the list, as shown in the slide. In addition, the list of AI developers "commit to implementing the Hiroshima Process International Code of Conduct" will be published later on the same Hiroshima AI Process website.

On July 19, 2024, the OECD launched the pilot phase of the "Reporting Framework for the International Code of Conduct for Organizations Developing Advanced AI Systems" and invited voluntary participation online. The deadline was September 6, and the survey results are expected to be published later on the same website. I expect that further details, including the official launch of the Reporting Framework, will be decided at the next round of the Industry, Technology and Digital Ministerial meeting on October 15. As a deliverable of the Hiroshima AI Process, the "Hiroshima AI Process Comprehensive Policy Framework" was presented with the following four elements on the slide: (1) the OECD report "towards a G7 Common Understanding on Generative AI", (2) international guiding principles for all AI actors, (3) international code of conduct for AI developers, and (4) project-based cooperation on AI, which envisages cooperation with existing and new projects and initiatives on generative AI worldwide.

The OECD report includes the results of the questionnaire sent to G7 members to identify common policy priorities for generative AI. It shows that all G7 members considered "disinformation and the associated manipulation of opinions" as the dominant risk. In terms of cyber, the 3 countries saw "threats to cybersecurity" and "threats to illegal activity" as the risk, respectively[1]

And all G7 members felt that the "responsible" use of generative AI technologies was the most URGENT and IMPORTANT priority from a policy perspective. The subsequent discussion and drafting work in the working group was conducted with this result of the questionnaire in mind.

---

1 Q: What are the top five risks generative AI presents to achieving national and regional goals? (Figure 2.2 in the OECD Report).

The 2nd and 3rd items of the Comprehensive Policy Framework are almost identical in content, as the Code of Conduct is a more elaborate version of the Guiding Principles. The only difference between the two is the intended audience. The Guiding Principles are intended for all AI users, with 12 principles, 11 of which are taken from the Guiding Principles for AI Developers released in October. A new principle has been added for all AI actors, which calls on them to "promote and contribute to the trustworthy and responsible use of advanced AI systems."

Due to time constraints, I will only discuss the Code of Conduct today. The slide shows the list of actions and recommendations set out in the Code of Conduct, which organizations developing AI should follow.

1: Identification, Evaluation, and Management of AI risks (*) before deployment

Action no. 1: Organizations should "take appropriate measures throughout the development of advanced AI systems …… to identify, evaluate and mitigate risks across the AI lifecycle." Such AI risks include offensive cyber capabilities, and threats to democratic values and human rights, including the facilitation of disinformation or harming privacy. To this end, organizations should employ a variety of internal and external testing measures.

(same above) 2: Post-Deployment Monitoring and Reporting

Action No. 2: Organizations should "identify and mitigate vulnerabilities …… after deployment" through 3rd-party and user discovery and reporting.

(same above)3: Transparency Reporting

Action No. 3: Organizations should "publicly report advanced AI systems' capabilities, limitations, and domains of appropriate and inappropriate use, to support ensuring sufficient transparency, thereby contributing to increase accountability." Examples of such measures include transparency reporting.

(same above) 4: Incident Management and Reporting

Action No. 4: Organizations should "work toward responsible information sharing and reporting of incidents …… with industry, governments, civil society, and academia."

(same above) 5: Organizational Governance

Action No. 5: Organizations should "develop, implement and disclose AI governance and risk management policies" and improve employee familiarity with their duties.

(same above) 6: Information Security

Action No. 6: Organizations should "invest in and implement robust

security controls, including physical security, cybersecurity and insider threat safeguards across the AI lifecycle."

(same above) 7: Content Authentication and Provenance

Action No. 7: Organizations should "develop and deploy reliable content authentication and provenance mechanism, where technically feasible, such as watermarking …… to enable users to identify AI-generated content."

(same above) 8: Research and Investment to Advance AI Safety and Mitigate Societal Risks.

Action No. 8: Organizations should "prioritize research to mitigate societal, safety and security risks and prioritize investment in effective mitigation measures," which includes research on upholding democratic values, respecting human rights, protecting children and vulnerable groups, safeguarding intellectual property and privacy and avoiding harmful bias, misinformation, disinformation, and information manipulation.

(same above) 9: Advancing Human and Global Interests

Action No. 9: Organizations should "prioritize the development of advanced AI systems to address the world's greatest challenges" including the climate crisis, global health and education.

(same above) 10: International Interoperability and Standard

Action No. 10: Organizations are encouraged to "advance the development of and, where appropriate, adoption of international technical standards" and best practices, including for watermarking.

(same above)11: Data Input Measures and Protections for Personal Data and intellectual property

Action No. 11: Organizations are encouraged to "implement appropriate data input measures [to mitigate against harmful biases] and protections for personal data and intellectual property." As many of you may be aware, other AI governance initiatives were underway in parallel with the Hiroshima AI Process in 2023. In particular, the OECD released the update of the "AI Principles" in May[2], and the US government announced "Voluntary Commitments from Leading AI Companies to Manage the Risks Posed by AI" in July[3].

As I don't know what the discussion was within the working group, which took over 100 hours, but given the similarity between these documents, it seems that the drafting work of the Hiroshima Process Code of Conduct

---

2 AI Principles Overview - OECD.AI

3 On July 23, 2023, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI | The White House

was inspired by, or at least infused with ideas from the OECD AI Principles and the Voluntary Commitments by leading American AI companies as shown in the slide. As I explained earlier, the OECD conducted the pilot phase of the reporting framework for the International Code of Conduct for Organizations Developing Advanced AI Systems from July to September. The survey is intended to "monitor the voluntary application of the Code of Conduct by AI developers, and is structured around the 11 action items of the Code of Conduct, which total 48 pages. In addition to members of the G7 Working Group and OECD experts, AI companies and organizations from G7 countries were involved in drafting questions for the survey.[4]

Overall, the Hiroshima Process Code of Conduct is likely to have a positive impact on how AI companies manage risk in their products throughout the AI lifecycle. The Hiroshima Process documents are an ongoing process and are intended to be flexible, as they will continue to be reviewed and updated as technology advances and policies evolve.[5]

However, there seemed to be several outstanding issues that needed to be addressed. First, as stated in the December 2023 Digital & Tech Ministers' Statement, coordination and cooperation across multilateral forums[6] is key to achieving the goal set by the Hiroshima AI Process, which is to promote the safety, security, and trustworthiness of advanced AI systems internationally. The UN High-Level Advisory Panel on AI noted that more than 100 countries have not participated in any of the recent AI governance initiatives and suggested that "an inclusive policy forum is needed so that all member states ..... can share best practices."[7] The Hiroshima AI Process must seize the opportunity to reach out to more countries.

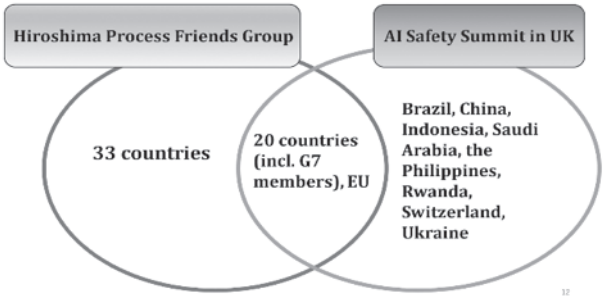
---

4 Canada: Cohere/France: Mistral AI/Germany: German Research Center for AI (DFKI)/Italy: iGnenius/Japan: Nippon Telegraph and Telephone Corporation (NTT), Nippon Electric Company (NEC)/US: Microsoft, Google, AWS, Meta, Open AI, Anthropic. G7、AI悪用リスクを監視　健全な活用へ世界共通基準 - 日本経済新聞 (nikkei.com) 2024年9月15日、

5 Para. 9, https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document02_en.pdf

6 Para. 11, ibid.

7 The UN high-level Advisory Body on AI, "Governing AI for Humanity: Final Report," 2024, p, 52, paras. 103-104, https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf



An example of such existing initiatives is the AI Safety Summit initiated by the UK government last year. As shown in the slide, 8 countries participating in the UK AI Safety Summit are not members of the Hiroshima Process Friends Group yet.

Finally, it is important to keep all stakeholders well informed about common AI risks and to promote as much common understanding as possible at the international level. For example, deepfake child pornography is a cybercrime in some countries, but not in others, even though the latter are parties to the Budapest Convention on Cybercrime. In this case, the risk perception of deepfake may vary from country to country. And such horrible content will circulate on the Internet forever. On the one hand, it's up to individual countries to decide whether to criminalize certain crimes, but we still don't know the big picture of generative AI technology. The Hiroshima AI Process documents take a risk-based approach. This means that the AI governance framework may change depending on the risk perception at some point in the future. Therefore, with these changes in mind, the discussion on what is the right balance between opportunities and risks should continue.

Massimiliano Signoretti
Lieutenant Colonel in the Italian Air Force, Legal Advisor Network Operations Command, Defence General Staff

Thank you very much for this opportunity to speak at this prestigious event. I am standing in for Dr Imogen Schon, Deputy Director of the Safety Institute of the UK Ministry of Science, Innovation and Technology. I'll start by talking about an approach to Artificial Intelligence and new technological frontiers that is innovative compared to others.

The UK's approach differs from that of the European Union. It doesn't focus so much on the immediate regulation of Artificial Intelligence systems and their use, but rather on governing and controlling the trajectory of a phenomenon that is disruptive to citizens' lives. This approach involves the creation of a Task Force of Artificial Intelligence experts at a global level, with the initial role of advisory board within a governmental structure. This board then evolves into a High Safety Institute, which defines an approach aimed at understanding and governing potential and risks.

We start from the observation that we do not have full knowledge of the development possibilities of new Artificial Intelligence models. Well-known applications such as ChatGPT or GPT-4 illustrate only a part of its capabilities. Personally, I have found tools such as Gamma AI to be extraordinary, for example, for creating slides and presentations in a short time. Managing these applications means starting from the recognition that Artificial Intelligence is not only negative: it has enormous advantages, such as the early prevention of certain diseases and the development of quantum computing.

However, there are also significant risks, such as the ability of Artificial Intelligence and quantum computing to break cryptographic codes within 5-10 years. This creates phenomena such as data harvesting, with the massive subtraction of data from databases for a future in which such information can be decrypted. The UK approach also aims to exploit the potential of these technologies through the establishment of test and evaluation laboratories, concentrating the ability to understand and govern risk at a governmental level.

In this context, DARPA, the US defence advanced research agency, has classified the development of Artificial Intelligence in three waves. The first is based on learning from large amounts of data to generate output; the second uses probabilistic algorithms; the third, currently in progress, concerns adaptation to contexts, with systems capable not only of learning but of understanding relationships between data, influencing decisions and processes.

Looking at the international scene, a dual approach emerges: exploiting the opportunities of Artificial Intelligence and managing the risks. NATO, for

example, has already issued specific strategies, updated in 2024 with the creation of the DIANA (Defence Innovation Accelerator for the North Atlantic) agency to accelerate knowledge in the technological field. The European Union has also adopted regulations, classifying Artificial Intelligence according to risk and prohibiting applications that compromise fundamental rights, such as the profiling of individuals.

A central issue is sovereignty. International law is strongly linked to the principle of territoriality and the behaviour of states, especially those with autonomous capabilities, can violate it. The Tallinn Manual explores how international law applies to cyber operations, identifying three types of offence: physical entry into a system, remote access and political interference, the latter being particularly critical due to its effects on elections and political decisions.

The use of autonomous capabilities and Artificial Intelligence poses significant problems, especially in determining the link between cyber operations and state responsibility. Psychological elements, such as the intention to interfere in the internal affairs of another state, further complicate the attribution of responsibility.

At the regulatory level, Artificial Intelligence capabilities intended for military or security purposes are often excluded from general regulation, both in the European Union and at the national level. However, such exemptions must respect fundamental rights and constitutional principles.

Finally, the International Committee of the Red Cross does not totally oppose the use of autonomous capabilities in armed conflicts, as long as principles such as necessity, distinction and precaution are respected. For example, it requires the maintenance of human control and the implementation of kill switches to interrupt operations when humanitarian principles are at risk. Geofencing and the prevention of the indiscriminate spread of software are also essential requirements.

DEBATE

Massimiliano Signoretti:

If there are questions, I am happy to answer them, to try to answer them.

Giovanni Salvi:

Thank you. Colonel Signoretti's presentation on the point about the use of instruments that still require the presence of man but are capable of self-determination in conflict situations is very interesting. Don't you think that the serious problem is that this situation must be bilateral? Because, if one of the two operators does not use instruments that can be controlled, thus losing a substantial part of the advantage - because the advantage lies precisely in the non-existence of human intervention, which makes it possible to exploit the great speed of decision-making and the greater precision of decision-making compared to the human one of the artificial instrument - well, the presence of the requirement for human intervention makes it less competitive. Won't this, in a conflict situation, lead, as it did in previous wars, to a very strong increase in the use of these tools instead? Do I make myself clear?

Massimiliano Signoretti:

Yes, Dr Salvi. Yes, this is definitely a problem. But it is a problem that starts before these autonomous capabilities are deployed in an operational theatre; it starts from the moment we conceive and train cyber autonomous capabilities, where we train artificial intelligence. Because when we train these capabilities, we insert within the instructions basically, which are given to these systems, the codes and limitations that come with being part of democratic systems.

So it is true that we are then confronted, eventually, with countries that do not have this attention to integrating, within the training of their artificial intelligence systems, democratic principles and fundamental values. But I don't think we can compromise on this, and so we must somehow try to bridge this gap, perhaps by always being, as NATO intends to do and as NATO states, able to maintain that "edge", that technological advantage, over our adversaries. I don't know if I answered your question.

Carlo Nordio:

Let me understand.

It is on the subject of liability. Is it possible for an artificial intelligence, self-cloning, creating - that is, a programme that may not have been foreseen by those who entered the initial algorithms - to enter another person's system, capturing and perhaps altering sensitive data? And if this were to happen, whose responsibility would it be?

Since the brain, the artificial intelligence, is not criminally liable, perhaps it would be civilly. But capturing sensitive data, or even altering it, would be a very serious risk. It is certainly a crime if committed by a human person. But in this case there is the possibility that the creator of this artificial intelligence will say: "No, it got out of hand, I didn't want to, it did it all by itself."

Massimiliano Signoretti:

Surely the capacity is there. The capacity is there. This is part of the training programmes and the Safety UK Institute.

This also applies to questions that are asked of artificial intelligence systems to train them to certain answers, but this is the difficult part. It also includes training them to what answers are undesirable. So, this is part of that programming mechanism. It is clear that a system that is capable of self-determination, if that fundamental element of human control over the process - even if it is "out of the loop" - is missing, but still maintaining control, this is possible.

We have seen this with a propagation, an uncontrolled proliferation of malicious codes. This happens. From a legal point of view, notwithstanding the difficulties of collecting digital evidence, which then clearly traces back to the author, whoever ultimately designs or employs the capability bears responsibility for the effects, even undesirable ones, produced by the use of that capability.

Clearly, bearing in mind that the psychological element is relevant in some crimes and not in others, it will always depend on the study and analysis of the case. If this provides for a psychological element, then that is one thing. If, on the other hand, there is objectivity in the harm, then it will have a different value.

Giovanni Salvi:

I can only add one thing to Colonel Signoretti's very clear answer. Yes, it is possible to transform the information content inside an apparatus. It has

been possible for some time and it is possible even with very simple apparatus, with injections of malware. This is a very serious problem.

The latest regulatory changes provide for the possibility, in undercover operations, not only of the apprehension of the computer object being attacked, but also its manipulation. This issue arose already in 2016, when I was Attorney General at the Court of Appeal of Rome and, therefore, I had the role of Giuseppe Amato. We then agreed with the intelligence apparatus that the use of malware and Trojans was, as far as authorisation was concerned, limited to listening only and did not include apprehension activities.

This is an extremely important issue, because from a judicial point of view it implies the need for certainty of the data acquired, which could be manipulated. At the same time, however, it is a very strong tool: for instance, a correspondence in a terrorist organisation could be altered in order to trap or blow it up.

The problem is huge, and I am glad it has come up, because I hope it is one of the things we will talk about in the coming days.

Stefano Lucchini:

Thanks also for the questions.

Thank you, Colonel Signoretti. Congratulations, really very clear, precise, to the point. The subject is absolutely fascinating. It is also that of democracy, to all intents and purposes, both from exogenous factors - which are the most dangerous - and, equally, from endogenous ones.

ENFORCEMENT OF CRIMINAL JURISDICTION IN VIRTUAL SPACE

Paola Severino

President of the Luiss School of Law and Professor Emeritus of Criminal Law at the Luiss Guido Carli University - former Minister of Justice - FVO Scientific Committee

Good morning, everyone,

I greet all the authorities present and, in particular, the Minister of Justice Nordio, with whom I share this panel, as well as all the authoritative speakers.

Let me also express my sincere thanks to the Occorsio Foundation and, in particular, to Prosecutor Salvi, who, with truly extraordinary commitment and passion, has taken on the organisation of this important collateral meeting to the G7, which brings together eminent representatives of institutions, international organisations and the academic world to discuss a truly central and pressing issue in the current scenario.

The enforcement of jurisdiction in virtual space is indeed a complex issue that has kept legislators and legal practitioners globally engaged for several years now and that, moreover, in the light of the incessant development of new technologies - and, in particular, of Artificial Intelligence - requires further, punctual reflection. With particular regard to the subject I have been entrusted with - that is, the application of criminal jurisdiction - it is well known how the typical characteristics of cyberspace - such as, for example, transnationality, aterritoriality and anonymity - make it very complicated to identify the State - or the States - in whose jurisdiction the offence falls. If, in fact, from the point of view of abstract activities, of delimitation of jurisdiction, national legal systems do not find significant limits in international law, far more relevant problems arise when faced with the activation of a plurality of state punitive initiatives.

The Italian Criminal Code, in Article 6 - similarly to what is provided for in many other legal systems - is inspired, as is well known, by the criterion of universality, in defining when an offence can be deemed to have been committed in the territory of the State. Moreover, the case-law of legitimacy has consolidated the orientation that considers sufficient to establish Italian jurisdiction the commission in the territory of the State of even only a fragment of the conduct, understood in a naturalistic sense, and, therefore, of "any act of

the criminal process, albeit lacking the requirements of suitability and unequivocalness required for attempt", provided that it is not a generic intent, lacking concreteness and specifity[8].

The tendency of national legal systems, moreover, to extend jurisdiction also to acts committed outside the territory of the State is stimulated by the provisions of some international Conventions, also on cybercrime. Suffice it to think of the provisions of Article 22 of the 2001 Budapest Convention. Even the new United Nations Convention on Cybercrime - about to be adopted by the General Assembly - allows States Parties to base jurisdiction, to an even greater extent, on acts committed outside their territory, for instance if perpetrated to the detriment of the States themselves, or their citizens, or in the presence of certain hypotheses of connection, provided that no acts are committed abroad that call into question the jurisdiction of other countries (Articles 22 and 5 of the Convention). Moreover, there is a real possibility that computer crimes may be transnational offences, if they meet the requirements of the 2006 Palermo Convention and Law No. 146 of 2006. In particular, the link between the activities of organised criminal groups, even operating in more than one State, and cybercrime is becoming more and more incisive, as has also recently emerged from the investigations carried out on the so-called cryptophonies, and on which the Unified Sections of the Supreme Court have pronounced themselves in the last year.

Precisely with regard to transnational offences, Article 15 of the Palermo Convention provides a further legal basis for extending the jurisdiction of States Parties to offences committed outside the territory of those States. Such provisions, together with the illustrated difficulties relating to the identification of the *locus commissi delicti*, make the possibility of the opening of parallel criminal proceedings not remote, from which there may be highly negative effects in terms of the exercise of the right of defence, the taking of evidence, the protection of the offended persons, and full compliance with the guarantees of due process. The resulting extreme remedy is therefore excessively late and unsuitable to avert these prejudicial effects. As a matter of fact, several years ago the United Criminal Sections already emphasised the notion of lis pendens, which is irrespective of the formation of a judgement, accepting an extensive interpretation of Article 649 of the Code of Criminal Procedure, understood as "the expression of a broader principle, which, even in the absence of an irrevocable judgement, makes the duplication of the same trial

8 Ex multis, Cass., Sez. VI, 27 marzo 2024, n. 13063; Cass., Sez. VI, 21 settembre 2017, n. 56953, P.M. c. G.; Cass., Sez. III, 2 marzo 2017, n. 35165; Cass., Sez. VI, 24 aprile 2012, n. 16115; Cass., Sez. VI, 7 gennaio 2008, n. 1180, L.

incompatible with the founding structures of the procedural order"[9]. However, instruments aimed at preventing and resolving conflicts of jurisdiction between states are still ineffective. In the areas of cybercrime and transnational crime, respectively, Article 22 of the Budapest Convention and Article 15 of the Palermo Convention identify consultation mechanisms in the event that more than one state party intends to exercise jurisdiction over the offences covered by the same treaties, or has already initiated proceedings. The new UN Convention on Cybercrime also confirms this type of approach (Art. 22). However, these are not very pregnant provisions, which - by not identifying modalities and possible outcomes of the contact between the different countries involved - risk failing to avert the effects of the opening of parallel proceedings. Similar criticisms can be referred, in the more restricted context of the European Union, to the procedure for the settlement of conflicts of jurisdiction outlined by Framework Decision 2009/948, due to the non-binding nature of the mechanism it regulates and the absence of a specific and punctual determination of the possible solutions it can lead to. It is, in short, a regulation that places certain "procedural" obligations on the countries concerned, with the intervention of Eurojust, but not the obligation to reach a result: in the event of failure to reach an agreement, in fact, the ultimate remedy of the prohibition of bis in idem may operate.

The problem of identifying the most suitable state to prosecute the crime, and the need to avoid parallel proceedings, are also behind the recent proposal for an EU regulation on the transfer of criminal proceedings of 2023. The proposal fits in with the objectives set out in the EU Strategy 2021- 2025 to combat organised crime and seems undoubtedly useful, considering also that the Council of Europe Convention on the Transfer of Proceedings in Criminal Matters of 1972 has been ratified by only thirteen states, and that the Agreement between the Member States of the European Communities on the Transfer of Proceedings in Criminal Matters of 1990 has never entered into force, perhaps due to the lack of attractiveness of an instrument that could place limitations on the exercise of jurisdiction. In the development of the negotiations, the importance of combining the effectiveness of the repression of offences that increasingly transcend national borders with the safeguarding of fundamental rights, such as the right to an effective judicial remedy and respect for the prerogatives of the defence, was also noted.

The transfer of criminal proceedings, with reference to the offences covered therein, is also provided for by the new UN Convention on Cybercrime (Art. 39): the provision is intended to be the legal basis for the transfer

9 Cass., Sez. Un., 28 giugno 2005, Donati.

itself, when no other treaties are in force between the states parties regulating this profile.

Precisely because of the uncertainties surrounding the determination of jurisdiction, it is essential that the authorities of the individual states cooperate effectively in preventing and combating cybercrime. A virtuous example in this regard is what is provided for in the NIS (Directive 2016/1148) and later NIS2 (Directive 2022/2255) directives. I refer, in particular, to the establishment of the collaboration group, the "CSIRT" network of intervention points and, most recently, the EU CyCLONe (*European Cyber Crisis Liaison Organisation Network*). While the collaboration group can play a significant role in terms of exchange of information and best practices, sharing of intervention strategies, and joint risk assessment, one of the tasks of the "CSIRT" network is precisely the implementation of a coordinated response to a cyber incident within the jurisdiction of a Member State, or of a cross-border nature. also CyCLONe can support the identification and management of measures to deal with such incidents. Essential, in these areas, is therefore the work of the agencies: first and foremost, the European Cybersecurity Agency - whose operational role has been strengthened by the Cybersecurity Act (Regulation 2019/881) - and, in our country, the National Cybersecurity Agency, established in 2021.

The importance of a coordinated intervention of state authorities in the management of cyber incidents and threats is also reflected in the proposed European Union's *Cyber Solidarity Act*, presented in 2023, which envisages the introduction of special emergency management and incident review mechanisms, especially in order to deal with large-scale and high-impact offences.

Finally, I would just like to mention the recent approval of relevant supranational legal acts, which are a response to the uncertain definition of the boundaries of state jurisdiction in cybercrime matters and the need to capture electronic evidence across national borders. I am referring, in the context, to the EU the Regulation (2023/1543) and the Directive (2023/1544), which, five years after the presentation of their proposals by the Commission, introduced the instruments of the European production order and the European preservation order for electronic evidence. This is an innovative dimension of mutual recognition, based on direct contact between the judicial authority of one Member State and the service provider, holder of the data, established in another Member State. These measures aim to make the detection of offences more effective, although there is no shortage of critical aspects, such as the variability of the preconditions that may justify the order in the different legal systems, and the foreseeable difficulty for the service provider to

whom the order is addressed to assess its legitimacy.

A similar approach also characterises the Second Additional Protocol to the Budapest Convention on Cybercrime, which also provides for a direct cooperation procedure with the service provider established in another State party to the Convention for the acquisition of different types of data. Significantly, the protocol has also been signed by states that are not members of the Council of Europe; some provisions on the subject have also been included in the new UN Convention, to which I have already referred (Articles 42 and 43).

The hope is that the difficulties in the delimitation of state jurisdiction, in relation to cybercrime, will not lead to an unnecessary and detrimental multiplication of punitive initiatives - the result of an unwillingness to give up a fundamental expression of sovereignty - but will instead be the starting point for the development of an effective coordination of prevention and repression activities, starting with the European Union. Only by continuing along this path, in my opinion, will it be possible to meet the often unpredictable challenges that cybercrime will continue to pose, even in its cross-border dimension. To these challenges we must counterpoint cooperation between states, because the challenge will only be won, the battle will only be won, the war will only be won if states cooperate with each other and do not compete, in a misunderstood sovereignty key, for the start of criminal proceedings that, by duplicating initiatives, would make them less effective.

FIRST SESSION

JURISDICTION, RESILIENCE AND ACTIVE DEFENCE. WHAT EFFECTIVENESS IN VIRTUAL SPACE?

JURISDICTION, RESILIENCE AND ACTIVE DEFENCE. WHAT EFFECTIVENESS IN VIRTUAL SPACE?

CHAIRPERSON

Alessandro Pansa

Former Director of Dis and Chief of Police - Special Advisor AI FVO

As we have heard from this morning's reports, the issue of security in Virtual Space is of concern to governments of all countries, and the attention being paid to the subject in international fora underlines its importance.

There is no doubt that AI is already changing our lives and will do so more profoundly in the future. We are living a different reality today, we are also living the so-called virtual reality. This is a new space in which we will have to live and coexist, for which we need rules. Virtual Space needs its own legal system. And Jurisdiction is the main basis for defining the system of rules. However, this need, which I would say is completely logical and clear, clashes with the complexity of the reality that was well presented to us in the various speeches that opened the conference.

I will not repeat them, nor will I delve into the challenges that AI poses to us and the threats it may pose. I just want to emphasise the importance of regulation. A few days ago, I attended the XIV Trans-Regional Seapower Symposium, in Venice, on the theme "A spotlight on the depths: the Underwater as the new frontier for humankind". It was attended by the heads of the navies of 69 countries, representatives of all international bodies dealing with the sea, academics and industry interested in the sector. They all emphasised that the Underwater domain is a new reality, ranging from the sea surface to the seabed and subsoil, 80 percent of which is unknown, and which attracts everyone's interest because it offers opportunities for development (suffice it to say that the marine subsoil contains the vast majority of the Earth's rare earth and mineral resources). The also Underwater, like Virtual Space, needs rules, otherwise the strongest and most unscrupulous will appropriate it to the detriment of everyone else. Between national and multinational powers, there will be no more than 10 players.

Virtual Space presents the same problem; the sooner a regulatory framework is created, the sooner it will be possible to frequent it freely. If there are no rules - I stress shared rules - strong actors, both state and private, will take possession of it and leave the less strong actors on the sidelines. I am sure that

the continuation of today's work will enable us to understand how to meet this challenge. Finally, allow me to bring a doubt of mine to your attention.

I am quite confident that the issue of jurisdiction and also that of the best forms of international judicial cooperation will be resolved at the conventional level. Of course, it will not be easy: but the intelligence of jurists combined with diplomatic skills will certainly lead to drawing a perimeter within which the judge will be able to exercise jurisdiction. The question I ask myself at this point is: will we be technically capable of carrying out the concrete actions that serve both the investigative and the trial level for the acquisition of evidence?

International legislation, such as that proposed by the EU last spring, will, for instance, determine what will be permissible for some, such as the acquisition of personal information by companies, but permissible for others, for instance in preliminary investigations.

Remaining with the example of privacy, the fundamental issue to be resolved will be: who holds the information? Who holds the technology to manage this data? Who will be able to protect it? will the various judicial authorities be able to implement their activities with the appropriate technology needed to do justice?

It is important that we all remember that we cannot simply ask ourselves the question of what principles and rules will govern jurisdiction or the taking of evidence. We must also ask ourselves the question: what will we be able to do to follow up on the rules that will be enacted? Will we have the technology that will enable us to ensure the proper application of the rules laid down? Will we have the technology to ensure the acquisition of evidence?

We are a country that does not produce microchips itself, does not produce complex hardware, in short, in the technology sector we are essentially dependent on foreign supply (a bit like energy sources). This technically puts us on a weak footing. It should be added that in addition to the industrial deficiency, there is also the circumstance that the big players in the sector, the so-called OTTs (over the top), are all foreign, mainly American and Chinese, but not only. We must be aware that if - for example - the perpetrator of the crime were an OTT residing abroad, if international treaties were to give us the possibility of trying one of these companies in Italy, with what tools will we present ourselves at the headquarters of that company or rather at its premises to acquire evidence? Will we have the tools to enter their systems, to probe their databases? Will we be able to access the applications indispensable to understanding how they committed the crime, and will we have the technologies to acquire forensic evidence?

I believe we have an answer: AI is the problem, but also the solution, since there is no such thing as evil or criminal AI, but there are evil people and criminals who can use it. So I am convinced that, knowing that there will never be an absolute level of security, behavioural limits and rules to be applied in Virtual Space will have to be identified and adopted collectively.

PRESENTATION BY THE MINISTER OF THE INTERIOR

Matteo Piantedosi
Minister of the Interior

Thanks to Alessandro Pansa for introducing the important topics of this debate, which is very topical and interesting. I start with a consideration: just a few days ago, the Royal Swedish Academy of Sciences awarded the Nobel Prize in Physics to Geoffrey Hinton, whose studies paved the way for modern artificial intelligence.

The thing that struck me was that the new Nobel Prize winner, in numerous public statements following this recognition, wanted to issue a strong warning about the risks of malicious use of this new technology. And this is because, as I believe was also amply stated in Alessandro Pansa's introduction, the advent of artificial intelligence is probably marking the beginning of a new era, full of exciting opportunities.

I very much agree with what he said: for opportunity, for our well-being, but also for a number of threats. So, it is a great opportunity, but also an issue about which we have to be very careful. Threats to our societies, which are occurring at a rate unknown in the past.

I feel the duty connected with the fulfilment of the institutional responsibilities that derive from my office, to fully exploit all the potential that this technology can guarantee in enhancing security, but with the possibility of protecting the exercise of individual and social rights. Precisely on this paradigm, therefore on the paradigm of the opportunity, but at the same time of the need for protection, during the meeting of the G7 Home Affairs Ministers held last week, I had the opportunity to promote a debate on the best strategies to make the digital ecosystem safer and also to ensure an ethical use of artificial intelligence. I have to say that with colleagues from the member countries of that G7 format, we had a concrete discussion on the main threats to our system of democratic values, noting and noting how these threats are expressed in a detrimental way in the real and digital world.

The subject of concerns related to the emergence of artificial intelligence does not only concern the virtual world, but also its repercussions in the concrete world. A first topic of discussion was certainly everything concerning the risks to our societies arising from international crisis scenarios. Obviously, the ones we are most interested in these times are the war theatres of Ukraine and the Middle East. It has been highlighted how there is an aggres-

sive and incessant jihadist propaganda spread on the web, and that this represents one of the major causes of radicalisation of individuals responsible for attacks on European soil. And so I think this already gives the idea of how, from the virtual, everything can then be transferred to the real world, to the concrete world.

In addition, on this occasion, we paid attention to the means of combating malicious interference, an issue known, therefore, to disinformation. On this we made precise commitments, also in the final declaration, to protect our democracies, especially during this delicate phase of electoral competitions. This is because it was agreed that we cannot passively witness the unscrupulous actions of malevolent actors who, making use of the increasingly aggressive use of, for example, deep fakes, attempt to undermine the elements of social cohesion in liberal societies, weakening citizens' trust in democratic institutions and the media.

One of the most novel elements that, as the Italian presidency, we wanted to put on the G7 agenda concerns the new frontiers of financial investigations to counter the illicit use of cryptocurrencies, on which I believe our country has cutting-edge experience.

A fruitful exchange of ideas arose on this specific issue, which gave me great satisfaction, both with all the G7 ministers, but especially with my American colleague, Deputy Attorney General Lisa Monaco, who was present at the meeting. We noted the difficulty of bringing to justice individual perpetrators of crimes who hide behind the anonymity of the web and who are protected by jurisdictions that are not always cooperative. We agreed, as Home Affairs Ministers, that the way forward cannot be other than to act preventively, i.e. through careful monitoring on the web and, subsequently, through the confiscation of illegal proceeds.

This theme of preventive action recurred a great deal in all the topics we put on the agenda, talking about the problem of cybersecurity in general and the various problems linked to the spread and risks of artificial intelligence. There was also a lot of talk, in the final statements, about artificial intelligence, and that this advanced stage of defence absolutely must pass through the involvement of private actors: internet providers, the big players that are present in the world of production and dissemination of digital products, and therefore that there must be a great alliance between public institutions and private institutions, which are in some way present in global scenarios.

It is a strategy that we also intend to strengthen in preventing and combating the spread of synthetic drugs, particularly fentanyl, which is increasingly traded on the dark web. This, again to give a sense of how cybersecurity issues do not end in the digital world, but have repercussions on

phenomena that affect the real world, even in traditional terms. And in this field alone, we also agreed on the American experience, where the issue of the spread of synthetic drugs is much more topical. In Europe it is a strong concern at the moment, but in America it is already very, very challenging. It was agreed that only targeted computer-based investigations will make it possible to disrupt the supply chain and seize the huge illegal profits for the traffickers.

On this important issue, I will say that, again to stay somewhat with the national security issues that in some way pertain to the functions and institutional mission of the Minister of the Interior, although it may appear to be an area somewhat distant from the digital dimension, we believe that we must aim at an effective action of monitoring the web, also to dismantle the cartels of migrant smugglers, through actions of obscuring the sites and social pages that sponsor the Mediterranean crossings. An activity that we in Italy are already doing with our police institutions. This is because we cannot accept that criminal organisations offer their services like any tour operator, jeopardising people's lives and violating the prerogative of states to govern migration policies. The fight against the phenomenon of digital smuggling is one of the pillars on which the action plan against smugglers that we have approved is based.

The document adopted at the end of the work on the mandate from the G7 leaders in Borgo Egnazia sets out the main lines of action that we intend to pursue. With our Home Affairs Minister colleagues, we agreed on a basic principle at the time: in order to meet the challenge of making the digital world safer, we must stay one step ahead of criminals from a technological point of view. I also found this in a nutshell in the presentation given by Alessandro Pansa. To this end, authorities law enforcement must have full command of the information technology means to prevent the commission of crimes and thus be able to identify the perpetrators. And it is precisely the theme of the potential offered by new technologies that was the focus of the working dinner we devoted to artificial intelligence, enhanced by the contributions of internationally renowned guest speakers.

There was a very important contribution by OpenAI vice-president Anna Maccanio, who illustrated the incredible growth prospects of the computational capabilities of artificial intelligence systems. It was highlighted how, within a few years, we will be able to rely on software capable of autonomously performing complex operations that will enable us to predict future events and trends of relevant phenomena in all fields of knowledge more and more accurately. Then there was the contribution of the Director General of the European Commission, Roberto Viola, who highlighted the guiding principles of the new European regulation on artificial intelligence. He did so with

a view to the essential contents of this regulation, which mainly address the need for an ethical and responsible use of artificial intelligence. This is because, according to the European regulation that has just been adopted, technology can never be used to manipulate people or to attribute immoral social approval ratings to citizens, nor can it be used to affect the essential rights of the individual, such as freedom and the expression of thought.

Therefore, a regulation that, through these cardinal points and the more general one of the protection of privacy and the fundamental rights of citizens, has already given an orientation on what must be the framework of limits that must characterise the potential of the use of artificial intelligence. And precisely the centrality of the rights of the individual is one of the aspects that I personally have sought to highlight on all the occasions on which I have addressed the issue. This is because, in order to avoid dangerous application drifts, I believe that we must ensure that artificial intelligence never takes the place of our judgement.

The paradigm, beyond technological developments, must always be this: never imagine that a technology, whatever the development, can replace human elements, the elements of judgement, but that it can only act as a support to human judgement. Operators who will use technology, both in the medical and fields, will law enforcement have to be adequately trained, not only on the scientific ability to interpret technical and technological opportunities, but also to interpret and use algorithm data in an absolutely responsible manner, avoiding blind reliance on the tools made available to them and thus subverting, where necessary, the outcome of the computerised procedure.

As I draw to a close, I believe that this G7 has given us the opportunity to engage in a fruitful debate on the potential that artificial intelligence can provide in enhancing security and also in promoting individual and social rights. There are many fields of application that we have imagined for a concrete use of the infinite processing capabilities that this new technology can provide.

I refer, for example, to the possibility of mastering in real time the enormous amount of data entered by police forces, both nationally and globally, so as not to leave grey areas in which criminals can hide. Or, there has been talk of so-called "predictive policing", which, thanks to an in-depth analysis of risk factors, can make it possible to allocate the resources of police institutions more efficiently, enabling more effective, timely and targeted interventions. This, of course, with the aim and sole purpose of protecting citizens and reducing crime rates. Because, as I said, artificial intelligence could also be extremely useful to have a more accurate overview of the dynamics and causes of migration flows, and to have, for example, data from the countries most

affected by the phenomenon of migration flows and related phenomena. This would allow us to have medium- and long-term perspectives and to put in place effective tools to prevent and counter these flows.

Moreover, these are issues on which even our Prime Minister, or rather, especially our Prime Minister, had the opportunity to speak during the UN General Assembly in New York, an occasion on which Prime Minister Meloni pointed out how the international community must cooperate to prevent this domain from becoming a free zone without rules and how, conversely, it is necessary to set up global governance mechanisms that are capable of ensuring respect for ethical barriers.

INTELLIGENCE IN A CHANGING WORLD. THE DIFFICULT BALANCE BETWEEN RESILIENCE AND REACTION

Lorenzo Guerini
President COPASIR

In the *Annual Progress Report* presented in July of this year by the UN Open-Ended Working Group on Security and the Use of Information and Communication Technologies (ICTs), it is stated that participating countries have noted a worrying increase in the malicious use by some states of ICT-based covert information campaigns to influence processes, systems and the overall stability of other countries. Such conduct undermines trust, can trigger process *escalation* and can also threaten international peace and security, as well as cause direct and indirect harm to individuals.

In the 2023 report of the National Cybersecurity Agency, it is emphasised how the Agency's operational activities, both in the preventive phase of monitoring, threat analysis and alerting those exposed to risks, and in the reactive phase of incident response, have undergone a significant increase in numerical terms over the previous year, "indicative of a general increase in cyber activities, also noted at a European and global level". In particular, the data clearly show a significant increase in the number of reports addressed to the Agency and how, against a number of reports received substantially in line with that of 2022, the number of cyber events increased by about 30% and incidents more than doubled. I imagine, but Director Frattasi will be able to confirm this, that the trend for 2024 can only confirm the increase in the activity to which the Agency he directs is called upon on a daily basis.

Added to this is a considerable increase in geopolitical tensions worldwide, which makes the issue of cyber security particularly sensitive. The development of new technologies and the increasingly pervasive use of the Internet for all actions related to even the most trivial gestures of everyday life, as well as the growing use of artificial intelligence, have determined and will undoubtedly continue to determine a radical change in the very conception of threats by actors, both state and non-state actors, intent on perpetrating actions to the detriment of democratic countries such as ours, and even threats with the purpose of terrorism. Let us simply think of the damage that a cyber-attack can do to the network of a hospital system, blocking the provision of health services or potentially even taking control of instruments, the use of which is increasingly frequent, of telemedicine or precision robotic medicine.

Abstractly speaking, it would be easier today to carry out an air or rail attack by hacking into computer systems than by physically placing explosive devices or using hijacking agents. Or think of the panic that a breach of a banking system could create, paralysing the daily actions of millions if not billions of citizens.

We could say that cybersecurity rests on two equally fundamental legs: the first is that of the resilience of our information infrastructures, on which the ACN has been doing extremely important work since it was set up, which, even beyond responding to the growing number of events that occur daily, rests on a strategy that also includes a major effort to train individuals and businesses in the responsible and careful use of digital technologies. The other leg is that of the proactive reaction and prevention actions to which our services are called *intelligence* and whose perimeter has been drawn with precise stakes by the legislator. The simple considerations I have just made have direct implications for the ways in which our services *intelligence* react to or prevent threats that are constantly evolving and by their very nature difficult to pinpoint *a priori*.

The management of such operations, the adoption of which often has to take place extremely quickly to ensure their effectiveness, poses, in fact, obvious problems in several respects, from prior authorisation to subsequent control, up to the more jurisdictional issues, starting with territorial jurisdiction itself. In this regard, suffice it to think how, in the cyber sphere, nothing can be taken for granted as far as attribution is concerned. In fact, in order to trace the subject who has carried out an action or a threat, it is necessary to retrace the entire chain of the countless actions of automated machines, materially residing in different territorial spaces and often very distant not only physically but also from the point of view of the regulatory framework. This is where delicate issues of sovereignty and differences between legal systems come into play, often involving the competence even of states outside the subject (or the state itself) that perpetrated the attack and that of those who suffered it, simply because they hosted a piece of this virtual chain in their respective territories. Often the actions required to prevent or respond to an attack presuppose the adoption of conduct that in the country where the servers reside, or even in Italy, is or may be considered a crime.

These issues, and in particular the more strictly one's intelligence-related , have been remedied by the legislature with Decree-Law No. 115 of 9 August 2022, converted, with amendments, by Law No. 142 of 21 September 2022, containing precisely provisions on cyber *intelligence.*

The legislator of 2022, moreover in a scenario of full conflict in Ukraine, establishes with reference to the adoption "of measures of *intelligence* on

counter in the cyber environment, in crisis or emergency situations in the face of threats that involve aspects of national security and cannot be dealt with by resilience actions alone, also in implementation of obligations undertaken at international level" a substantial parallelism with the scheme, already tested in Law no. 124 of 2007, relative to the so-called functional guarantees. As authoritatively stated by Dr. Salvi, the basic assumption of this attribution of powers is that the attacks are relevant from a national security perspective. In particular, the values protected are those that can be traced back to the community State and that give life to the democratic republic, in the synthesis of the constitutional order, with particular reference to the profiles of the integrity of the territory and the sovereignty, internal and external, of the State. This clarification is important because it strongly circumscribes the field of conduct that, subject to the authorisation of the competent authority, may enjoy particular exculpatory guarantees precisely for the protection of vital state interests.

The provision, moreover, makes an important leap forward in prefiguring the adoption of law enforcement measures, which under Article *7-bis* of Decree-Law No. 174 of 2015, could be undertaken "in crisis or emergency situations abroad involving aspects of national security or for the protection of Italian citizens abroad, with the cooperation of special Defence forces with the consequent support assets of the Defence itself".

Article *7-ter* of Decree-Law No. 174 of 2015, introduced in 2022, with reference to law enforcement actions in the cyber sphere drops all geographical references and therefore also covers any law enforcement actions carried out within the territory of the Republic.

Precisely in view of the breadth and delicacy of the powers conferred by the rule, it provides that the entire system is to be governed by a provision of the President of the Council, adopted after consulting COPASIR, aimed at regulating the authorisation procedure, the characteristics and general content of the measures that may be authorised in relation to the risk to the national interests involved, according to criteria of necessity and proportionality.

The exercise of such actions of contrast therefore presupposes, on the one hand, a rigorous prior authorisation screening for the conduct exempted from criminal liability, and on the other, an explicit reference to the functional guarantees as outlined in Article 17 of Law No. 124. 124 of 2007, which expressly provides for rather stringent limits on the use of such exemptions, such as, for example, their exclusion in cases in which the conduct envisaged by law as an offence constitutes offences aimed at endangering or damaging the life, physical integrity, individual personality, personal freedom, moral freedom, health or safety of one or more persons.

On the other hand, the outlined procedure, by bringing such actions within the scope of functional guarantees, also entails a subsequent control by the Parliamentary Committee for the Security of the Republic, to which the President of the Council of Ministers must transmit communications relative to the conduct of the operations authorised on the basis of the aforementioned legislation. The Committee, in the face of such communications, although without entering into the dynamics of operations in progress, is always within its power to carry out all the in-depth investigations it deems necessary, through documentary requests or requests for hearings of the heads of the services intelligence . I believe that, especially in this context, the subsequent control that the Committee is called upon to exercise can be particularly important and significant.

Indeed, in a context that is constantly evolving, both in terms of the tools that can be used and in terms of the potential pervasiveness of the action of the services *intelligence* in areas of personal freedom, as well as in terms of the need for reactions that are if not instantaneous, at least very rapid, the existence of a democratic body to which it must be accountable is essential in balancing the interests at stake.

In this regard, one could open a wide-ranging discussion on the asymmetry between the various actors, both state and non-state, from systems different from our own and potentially hostile to us, which are not subject to the same democratic rules proper to our rule of law to which the apparatuses of democratic countries are fortunately obliged. Let us also think of the enormous amount of personal data held by powers such as China and the profound differences (to put it mildly) in the regulation of their protection, or the massive disinformation activities deployed by actors such as Russia. Our legal system requires, on the one hand, that law enforcement actions be carried out only when there are real and concrete national security needs and, on the other hand, that they respect a criterion of proportionality.

Finally, I would like to mention another sensitive issue that arises with regard to the recruitment of both those who are called upon to collaborate with activities related to the resilience of digital infrastructures, and, even more so, those called upon to carry out measures in the field in law enforcement the cyber domain.

In the IT sector, even more than in the sectors, traditional the technical profiles of individuals, ultimately called upon to play a role similar to that of the so-called *intelligence hackers*, are extremely attractive on the market of large technology companies and their mobility is decidedly high, without, of course, considering the hypothesis that they could be recruited by public or private subjects belonging to countries that are antagonistic in this historical

phase. In this regard, action must be taken to preserve the training investment and know-how acquired and also to protect our apparatus from the possible transfer of sensitive knowledge. Instead, I will not dwell on the more jurisdiction-related profiles because I am sure that they will be addressed with great competence by the other speakers, starting with Dr Salvi, who has great experience in the field.

However, I would like to associate myself with the invitation he himself formulated elsewhere to adapt the substantive and procedural instruments to the new dimensions of crimes committed in virtual space, in order to avoid the proliferation of conflicts of attribution between the powers of the State, when the need for investigation clashes with that of prevention. As we have seen, in the cybernetic sphere the spatial dimension and therefore the identification of territorial jurisdiction appears extremely blurred. The very effects of the measures adopted may be difficult if not impossible to assess a priori. Therefore, the only solution appears to be that of a regulatory framework that is as clear as possible in delineating the stakes that the State imposes in order to be able to allow the activation of the exculpatory measures, to be combined with a rigorous ex ante scrutiny by the political authority (President of the Council and Delegated Authority), responsible to Parliament for its conduct, as well as a scrupulous subsequent examination by COPASIR.

The application practice that will be formed in the coming months and years on these provisions will then also make it possible to open a reflection on the adequacy of a system that is called upon to strike a difficult balance between the need to provide immediate and effective responses to complex and often difficult-to-detect threats and the safeguarding of those values and principles, including those of a constitutional nature, that govern the exercise of such delicate functions of our security apparatus.

In this regard, the Committee that I have the honour of chairing will play its part without discounting, but always with a view to institutional cooperation, performing, also through the use of the instrument of reports to Parliament provided for by law, a stimulating function, in addition to the direct control function.

CYBER AS A TOOL OF INTERNATIONAL TERRORISM. NEW THREATS - NEW RESPONSES. THE PROBLEM OF ATTRIBUTION. SPECIFICITY OF ATTRIBUTION IN CYBERSPACE

Alessandra Guidi
DIS Deputy Director

Artificial intelligence and, in particular, generative intelligence, although a relatively recent manifestation of a technology that has existed for decades, is part of a heterogeneous and complex scenario, raising fundamental questions about the concepts of sovereignty, jurisdiction and territoriality. Its introduction has the potential to further destabilise existing paradigms, making the need for legal and political rethinking even more urgent. Indeed, these emerging technologies are profoundly changing the global regulatory and political environment, challenging the effectiveness of traditional regulatory tools and requiring an interdisciplinary approach to address their socio-economic and geopolitical implications. Artificial intelligence is, therefore, a key element in shaping the future geopolitical balance, favouring those nations that will be able to govern it with efficiency and foresight. It is not surprising, therefore, that major global powers, such as the United States, China, Saudi Arabia, and several other nations, are investing significant resources in the development and application of AI. The scale of investment in this field is not only about building technological capabilities, but also about creating an integrated ecosystem that supports innovation and control of this strategic technology.

Artificial intelligence, in itself, is not a radically innovative technology: its potential lies in the extraordinary amount of data available today and the increasing computational capacity. The availability of these two factors is expanding at a dizzying pace, raising the question of who actually owns the data and, consequently, de facto control of the algorithms that are "trained" on them. These data often do not belong to individual states, organisations or companies, thus introducing important geopolitical, economic and social implications. The ability to collect and use these tools in fact determines a significant competitive advantage at the international level, increasing the gap between the countries that have the resources (data and computational power *in the first place*, but also talent) to exploit these technologies and those that, instead, not possessing them, are excluded.

AI is thus based on two "pillars": the availability of so-called "*big data*" and an advanced computational capacity, factors that, as we have said, are rapidly becoming central in the global landscape. Suffice it to say that, by 2024, the number of Internet users will have reached almost 5.5 billion, corresponding to about two thirds of the world's population. In addition, the number of connected devices has exceeded 8 billion, helping to generate a volume of data that is crucial for training AI models. The proliferation of connected devices and their increasing ability to interact with each other without human intervention are creating a highly complex digital ecosystem in which the quantity and quality of available data is set to grow exponentially.

Such a scenario poses significant challenges to national and international security. The ability of artificial intelligence to process huge amounts of data in a very short time makes it an extraordinary opportunity, but also a potential vector or "facilitator" of very serious threats. A striking example is that of the so-called *deep fakes*: the ability to generate false, but highly realistic video content has already demonstrated its dangerousness: in addition to the increasingly insidious and verisimilar scams, think of the potential political, economic or public security impacts that could arise from the dissemination of, for instance, false statements by a political or government figure, going so far as to jeopardise political stability and trust in institutions.

Even seemingly more ordinary threats, such as *phishing*, are becoming increasingly sophisticated through the malicious use of AI, becoming almost indistinguishable from legitimate, real communications. These attacks are not only capable of deceiving ordinary individuals, but also of targeting the most structured organisations, with potentially devastating consequences. Furthermore, advanced algorithms can be used to analyse codes in search of vulnerabilities in computer systems, automating the search for targets. *Malware* with "self-training" capabilities pose a further danger: once introduced into a system, they are able to continuously improve their evasion and infiltration strategies. These considerations become even more topical and relevant when one addresses critical or sensitive infrastructures, such as healthcare infrastructures: an attack against even a single local healthcare company - on which several facilities, hospitals and health centres depend - can in fact have considerable impacts, with cascading effects that go far beyond the individual affected.

A further aspect that should not be overlooked is that the AI itself, as an algorithm, is attackable. This can be done in various ways: by "poisoning", for instance, the very data on which it is trained. This phenomenon is extremely insidious, since it entails the risk (in itself already intrinsic to the AI itself, since its internal decision-making processes are characterised by "opac-

ity") of introducing unexpected, misleading or even dangerous results, thus irreparably compromising its reliability: if the data feeding the algorithms are altered, the applications based on them will also be altered, with significant consequences on the *outputs* produced by these technologies that, it must be remembered, are and will be increasingly present and pervasive.

In this context, the concept of resilience becomes crucial: like the mother of Winnicott, the well-known British psychoanalyst and paediatrician of the last century, perfect security "does not exist", there is "good enough" security. Even with highly sophisticated defences, there is always the possibility that a threat will go unnoticed or that a particularly elaborate attack will overcome the protective measures. The important thing, and this is where resilience comes in, is to develop the ability to get back up, recover and react after the blow suffered, restoring systems to operability and ensuring continuity of services in the shortest possible time, minimising the negative consequences.

Consider, again, the example of the health sector: a successful attack, in such cases, could lead to the interruption of essential services and life-saving therapies, blocking emergency rooms, ambulances and operating theatres. And it is a phenomenon that affects not only Italy, but all the most advanced countries. For this reason, it is essential to implement measures that minimise the damage caused by an attack and ensure the fastest possible restoration of services.

With this in mind, the National Cybersecurity Agency (NCA) has adopted the concept of resilience as a guiding principle, with the aim of ensuring the timely recovery of compromised systems and thus also protecting national security in cyberspace. This translates, concretely, into operational practices ranging from the design of more robust systems to the training of specialised personnel, and the creation of coordinated response protocols involving both the public and private sectors.

Cyber resilience has recently received an important legal recognition through Law No. 90/2024, which, in addition to regulating more extensively the operational relations and information links between ACN, Judicial Authorities and Judicial Police, has introduced appropriate balancing mechanisms between investigative and national resilience needs, functional to ensure the effective and timely conduct of recovery activities, the assurance of evidence sources and the coordination of the National Anti-Mafia and Anti-Terrorism Prosecutor (PNAA).

In particular, the provision stipulated that the Agency must inform the NAPA of the news of an attack against certain computer or telematic systems and, in any case, when a Perimeter, NIS or Telco subject is affected, and that

the Public Prosecutor must inform the NAPA when he acquires news of certain serious computer crimes, also ensuring the information link with the CNAIPIC. In addition, the same law introduced specific mechanisms for balancing investigations and resilience, providing: on the one hand, that the prosecutor shall issue the necessary provisions to ensure that urgent investigations are carried out taking into account the activities carried out by the Agency for resilience purposes; on the other hand, that, in order to avoid a serious prejudice for the course of the investigations, the prosecutor may order the postponement of resilience activities with a reasoned order.

An emblematic case was the arrest of a young hacker, who was responsible for an attack on the systems of the Italian justice system: thanks to the cooperation between ACN, DNA, the investigating Public Prosecutor's Offices and the Postal Police, it was possible to secure the compromised systems without affecting the ongoing investigations, thus ensuring the continuity of critical services while respecting the investigative needs. This experience demonstrated the effectiveness of a coordinated and synergic approach to the management of security incidents - which are also crimes, but not limited to -, highlighting the importance of cooperation between the different institutions involved.

The cyber domain is a domain unlike any other: it is transversal, multifaceted and changeable. It is a domain in which we are all personally immersed. Consequently, it must be recognised that cyber resilience and security rest on the shoulders of each and every one of us: on every single company, on every single institution, on every single citizen. Only through a holistic approach, therefore, will it be possible, if not to eliminate it, then to reduce cyber risk to at least a "physiological" level.

For such an approach to be fully realised, it relies on a fundamental element: culture. We can spend millions of euros to secure systems, but if an employee does not take all the necessary precautions and, for example, while *smart working*, connects the service computer to the home network without precautions, every investment risks proving futile. Due to a lack of security culture, the overall effort of an entire organisation is thus thwarted. It is therefore crucial to invest in training and spreading awareness of cyber risks at all levels and in all sectors, especially with regard to the challenges and opportunities offered by new technologies in an increasingly digitised world.

In conclusion, returning to the topic of artificial intelligence, which is emblematic of the era we are living in, I would like to close by reiterating that AI offers extraordinary opportunities, but also poses enormous challenges, particularly with regard to national security in cyberspace, and beyond. In such a scenario, characterised by the spread of AI as a potential offensive,

defensive and attack platform, resilience will prove to be an even more crucial element in ensuring the stability and security of our country in the face of new, emerging or simply different threats.

The future of national security, but also that of our own security, will depend on our awareness and ability to integrate advanced technologies, develop effective defence and resilience strategies, and ensure that responses to attacks are coordinated and proportionate to threats. Ultimately, resilience, enabled by culture, is not only a defensive strategy, but also a key component of a country's ability to thrive in an increasingly digitised and interconnected environment.

ACN (NATIONAL AUTORITHY FOR CYBERSECURITY) AND THE SAFEGUARD OF THE NATIONAL SECURITY IN VIRTUAL SPACE

Bruno Frattasi
Director of the Italian National Cybersecurity Agency

A brief but necessary introduction.

Looking at the latest developments in the speculative debate on the definition of national security, precisely on its content and limits, the current dramatic climate of belligerence has had a strong influence. For some time now, aspects concerning the preservation and stability of certain assets and interests, especially public ones, have been brought back to national security and made part of it, according to a vision that is excessively broad and, for this reason, such as to distort the authentic essence of the concept. There is no doubt, however, that whatever the configuration of the concept of national security that we assume, the cyber dimension, which has come to be added to the political-institutional, economic-financial and energy dimensions, occupies an ever-increasing weight within it. All of them, each and as a whole, concern and call into question the safeguarding of the national political community, with the common objective of protecting citizens, institutions and businesses from any attempt at interference, interference or pressure, whether internal or external, that might even compromise the continuity of the country's life, undermining its freedom and self-determination.

The same terms, with a strong reference to the essential functions of the State, are also expressed in Article 1 of the law that instituted the Cyber National Security Perimeter five years ago. It seems evident, therefore, that national security is interpenetrated with the principle of sovereignty, understood in the classical sense of plenitudo potestatis; so that national security, in virtual space, is presented - first and foremost - as a predicate of national digital sovereignty. But we are dealing, and have been for some time, with another form of digital sovereignty, the European one. An "imaginative and highly evocative expression" that goes back to President Von der Layen's speech the state of the Union in 2020.

As has been noted, this expression - European digital sovereignty - contains a political and not a legal statement, indicates a goal to strive for and does not describe an already acquired and consolidated state of affairs. Above all, it is inscribed in a logic of competition and confrontation between global powers in which the national dimension is inevitably transcended, over-

looked, but, as I will attempt to clarify, by no means obliterated or eclipsed; so that even in this form, the supranational European one, digital sovereignty is still linked to national security, although it acquires a richness and strength that go beyond the domestic dimension alone, and which cannot be drawn on except in the context of the Union. My speech is aimed at illustrating, also by means of brief examples, how the Agency places itself at the service of national security, whether this remains functional to the affirmation of national digital sovereignty, or whether it is placed within the horizon of European digital sovereignty.

The Agency's contribution to national security has its secure anchorage in the already mentioned law establishing the National Cyber Security Perimeter. As we know, it was conceived and implemented to delimit - in the absence of a clear address in the first NIS directive - IT structures and surfaces (networks, systems and services) necessarily to be protected according to the highest standards of technological security, defined (and here the clarification is not a negligible form of legislator's acumen) "at international and EU level".

The Agency's activity is expressed here in a number of substantial moments: i) the first consists in participating in the process of subjective and objective definition of the Perimeter; participation that takes place by assuming a central role that is also declined in a function of coordination, according to the plot that the same provisions of the founding law of the Agency were charged with bringing to light after the introduction of the Perimeter, and taking care to establish the appropriate links between the two bodies of legislation. Incidentally, wishing to carve out its role with greater incisiveness coordinating, it is here the case to recall what the Agency ordered the day after the outbreak of the Russian-Ukrainian conflict, when, in implementation of an urgent regulatory provision, issued in that climate it ordered all public administrations to follow a criterion of necessary diversification in the procurement of protection devices, in order to avoid forms of technological dependence that could have inappropriately exposed our digital surface to cyber risks and compromised national security itself; ii) another moment in which the peculiar function of the Agency is expressed with respect to the subjects as well as to the goods and services included in the Perimeter, concerns the activity of the National Assessment and Certification Centre, whose activity takes the form, in cases of particular complexity, of technological scrutiny of ICT goods, systems and services intended to be used in that part of the information surface included in the Perimeter, with the further consequence that the assessment, previously carried out, on the reliability of the new assets must also take into account the context of use, i.e. their scope of use, as the

rule clearly clarifies. Conditions and prescriptions may result from the assessment, which are then transfused into the procurement procedures of the entities belonging to the constituency of the Perimeter and form the subject of binding clauses included in the calls for tenders so that the most absolute respect of the indications given by the Agency is guaranteed; iii) the protection of the perimeter of national cyber security is also concretized in the establishment of very tight deadlines within which the subjects included therein are obliged to communicate to the Agency the impacts suffered by the part of the digital surface subject to such special protection.

Even more than in other areas, the immediacy of reaction and response to the incident appears fundamental here. Consequently, the interlocution to be established between the impacted subject and the CSIRT-Italy - the Agency's internal structure - cannot but conform to criteria and operational dictates of extreme promptness, capable of ensuring rapidity and precision of intervention. Therefore, the Agency's prior and punctual knowledge of the impacted digital structures, as well as of those who have full responsibility for them and who, for this reason, are called upon to dialogue and cooperate, once the incident has occurred, with the CSIRT-Italy, is essential. First with a directive issued by the Prime Minister in December 2023, and later with a law that partly replicated its contents by introducing them into the national legal system, particular emphasis was placed on the need - starting with the Perimeter Administrations - to refine and strengthen the collaborative aspects by urging public actors to prepare or update where they exist, incident response and management plans, and, in the event of an impact, to lend the Agency's operators maximum cooperation so that the restoration of full functionality of the compromised digital part takes place in the shortest possible time. In short, support and back-up activities are all the more likely to be successful the more the subject, towards whom such activity is deployed and provided, is willing to accept it, providing any necessary information on the cybersecurity organisation, also with regard to third parties involved.

Now, but here the discussion for obvious reasons of brevity can only be made in broad strokes, the advent of the NIS2 directive - the decree transposing is recent and will enter into force on 16 October next - will entail a major effort to strengthen the cybersecurity posture in many sectors, including those now covered by the Perimeter discipline. It will be a question of whether, precisely because of this broad protective umbrella represented by the new NIS framework, it is not perhaps more than appropriate to reconsider the configuration and current scope of the Perimeter, so that national digital security is even better specified and defined, thus coming to fully represent that ideal "safe" in which to store and guard the "crown jewels". And this also in order

to establish the most convenient reciprocity between the Perimeter system and the NIS system, to be considered more on a level of integration than of mere alternation.

It was said earlier that the defence of digital sovereignty passes through the ability to guarantee national security by preventing forms of interference that could lead to the loss of control of data or technology of strategic assets. From this point of view, it is worth dwelling on two engagement profiles of the Agency which, albeit from different angles, are nevertheless both demonstrative of the assumption mentioned in the introduction, regarding the reconcilability of national digital sovereignty with European sovereignty; in the sense that it is not that one should give way to the other, having somehow lost the prerequisite for its exercise, but in the sense that the former represents the brick, the layer of digital security on which, precisely, the latter can be well founded.

The ascent towards the supranational dimension cannot and must not correspond to the "sacrifice" of the national one, nor to its obliteration: weaker European countries and less guarantors of their security in the virtual space could only contribute to keeping Europe in a more fragile and vulnerable condition, as well as making it less present and influential in the global context. Let us take as an example, in this direction, the effort made to support the transition to the cloud of central and territorial public administrations, which has seen the Agency engaged in the qualification of the National Strategic Hub, the first cloud structure in the country to have been certified at the highest level of security, thus, able to host any type of data, including strategic data, as such relevant to national security. I am also referring here to the recent approval of the national certification scheme for cloud platforms, which precedes the definition and launch of the European scheme. Here the construction of a regulatory model for the EU digital market that avoids its internal fragmentation is indeed measured against the need to promote, in the competitive game, continental technological autonomy, but also, and above all, against the need to ensure full control of data, without distinctions or exceptions of any kind, a prerequisite for a real sovereignty of the national information heritage, of each nation.

The goal of a European sovereign cloud cannot, once realised, be other than to serve, and strengthen, the national security of the various Member States; which confirms that we are not talking about different and incommunicable demands, but rather about the same demand, seen, on the one hand, in the interest of the sovereignty of the individual country, on the other hand, in the European perspective, therefore, within the strategy of regional technological independence repeatedly indicated.

A further example, among others possible, of the Agency's contribution to the defence of national security can be drawn from the exercise of the special governmental powers connected to the application of the Golden Power legislation, after it came to include among the activities of strategic importance broadband electronic communication services based on 5G technology, as well as "goods, relations, activities and technologies relevant to cybersecurity", in the list of which the cloud is also included. To tell the truth, the Agency's contribution to the activities of the Coordination Group, which sits at the Presidency of the Council of Ministers with the task of instructing the Government's decisions, has also concerned areas other than, *stricto sensu*, cybersecurity, and has in fact also extended to other goods and relationships whenever aspects sensibly linked to digital were touched upon, confirming the enabling nature of cybersecurity and its transversal relevance. To provide a measure of this contribution, in 2023 the Agency expressed its opinion, also contributing to the decision to exercise veto powers, in about 30 per cent of the notifications submitted under the Golden Power legislation. This percentage has increased in the current year, covering almost half of the notifications at present.

In a specific case dealt with this year - an acquisition transaction involving the financial sector - the Agency requested that the binding requirements also include the preservation of the organisational measures adopted by the target company, including the maintenance of the location of the information assets on national, or at least European, territory, to protect the confidentiality, security and control of data, classified as sensitive. The extension of the rules on the control of the acquisition of strategic assets also to the cyber sector has shifted the focus to the procurement of goods and services insofar as they are the subject of certain contracts and only if the contractual counterparties are non-European suppliers.

In this wake, there is also the recent provision, contained in this year's Law 90, according to which a soon-to-be adopted presidential regulation will define the cases in which, in order to guarantee national security, preference will have to be given to proposals or offers that contemplate the use of reliable cybersecurity technologies. In the list of that trust, the provision includes, of course, Italian technologies, but adds those of countries belonging to the European Union or adhering to NATO. In addition, the implementing provision will be able to identify third countries with which the above-mentioned supranational entities and organisations have collaboration agreements on cybersecurity, protection of classified information, research and innovation.

The provision stipulates that the same decree should define the essential elements of cybersecurity that public administrations required to comply with

the CAD must consider for the procurement of IT goods and services when they are used in a context of use relating to the protection of strategic national interests. It is the same regulation that makes it clear that the term "essential elements of cybersecurity" is to be understood as the criteria and technical rules that together guarantee, with respect to the importance of the interests to be protected, the confidentiality, integrity and availability of the data to be processed. In this way, the request to affirm in sectors crucial to the life and integrity of the country the principle of technological independence and data sovereignty is reaffirmed.

The cyber threat is global and incremental, and is so in both a quantitative and qualitative sense. Attacks by cybercriminals on critical infrastructures are steadily increasing, especially in the economically richer parts of the world and where the expansion of the exposed digital surface is more substantial. The most feared threat is represented by ransomware, which is doubly insidious because it seriously compromises data security, the exfiltration and encryption of which is functional to extortion blackmail, and to a considerable extent also undermines economic security. For these obvious reasons, the ransomware phenomenon has been the subject, with the aforementioned Law 90, of a legislative intervention to strengthen the punitive response that has introduced severe tightening of penalties. But the worldwide spread of the threat and its worsening have led to the establishment of a vast international alliance, the Counter Ransomware Initiative, whose objective is to define a shared action plan capable of cohesively countering the phenomenon without any point of permeability or ineffective resistance that might foster the criminal chain, and this precisely by virtue of the substantial convergence of national containment and response policies.

This initiative, in which more than sixty countries cooperate, is followed with great attention by the Agency and represents, alongside its constant participation in the Brussels Tables and Working Groups, a significant and relevant part of its action at international level. In this as in other forms of multilateral cooperation, the principle of collective security seems to be emerging, even on the scene of virtual space, as a mutual guarantee of the integrity and independence of the countries that freely adhere to an alliance bond.

Certainly, the incremental nature of the threat to national security is also linked to the development of emerging technologies. Quantum technology and artificial intelligence stand out against this backdrop: the dual nature that they share allows us to say, however, that the positive exploitation of both can nourish and strengthen, make the response to the threat more incisive and effective. This is the most prospective field of endeavour to which a

structural and also operational change of the Agency will correspond, prefigured by the creation, provided for by Law 90, of the National Cryptography Centre and by the employment, within our Body, of military personnel also functional to the disengagement, within the Cybersecurity Nucleus, of the tasks deriving in the matter of cyberdefence from the Memorandum of Understanding signed with NATO. The integration between the civil and military components must be pursued and implemented with conviction, given the nature of the threat and its offensiveness multi-domain. Precisely because of this nature, because of the "fluidity" of the contexts in which it acts and its a- territoriality, it has always been characterised as a hybrid threat, with potential systemic effects.

In the presence of such a scenario, it would be impossible, but above all wrong, to think in a non-holistic way about national cyber security, i.e. in a way that did not consider, with due attention, the need for the closest cooperation between all the structures, including those of the intelligence community, deputed to this form of national security. Obviously, each one operating within its own role and according to its own mission.

INTERNATIONAL REGULATORY INSTRUMENTS. FROM TALLINN 2 TO TALLINN 3 MANUALS. FOCUS ON THE ROLE OF JURISDICTION

Marko Milanovich

Professor of Public International Law - Coordinator Tallinn Manual 3.0 - NATO Cooperative Cyber Defence Centre of Excellence

I am a professor of international law and not an authority in the Italian context, so I will offer an academic perspective on issues related to jurisdiction and developments in international law, with particular reference to cybercrime.

The concept of jurisdiction, in international law, refers to the power of a state, as a sovereign entity, to enact and enforce its own laws within certain limits, without violating the sovereignty of other states. This principle is central to understanding how international law adapts to new technological realities. The Tallinn Manual is an academic project, independent but supported by the NATO Centre of Excellence for Cyber Defence. It attempts to adapt existing international law, often centuries old, to the challenges posed by cyberspace. Since it is very difficult for states to agree on new treaties on the subject, the approach has been to reinterpret existing law to meet the new technological challenges. The first handbook, published in 2013, covered the application of law to cyberwarfare. The second broadened the scope to general topics such as sovereignty, intervention and human rights in the cyber context. Currently, work is underway on a third iteration, planned for 2027, which will update the handbook with practices developed in the intervening years.

Jurisdiction is only one part of the Tallinn Manual. There are various types of jurisdiction, such as prescriptive (the power to enact laws) and executive (the practical application of laws). The state may exercise jurisdiction over facts occurring on its territory or involving citizens or national interests, even if those facts occur outside the territory. For example, an offence committed against an Italian citizen abroad can be prosecuted by the Italian authorities. In the cyber sphere, the territoriality principle is complex. A crime such as hacking can occur simultaneously in several states: where it originates, where it is completed, and where the IT infrastructure involved is located. This makes the application of jurisdiction by more than one country possible. However, there are more nuanced situations, such as the mere transit of

data through third states, which raise questions about which jurisdictions can be exercised.

A recent example is the US indictment of five members of Russian intelligence for the use of the malware Whisper Gate designed to target Ukraine. Although the US had minimal connection to the crimes in question, it justified its jurisdiction based on the fact that US computer systems had been probed by the perpetrators.

Enforcement jurisdiction, i.e. the application of laws outside the national territory, is even more problematic. An action such as questioning a witness via video conference often requires the consent of the state where the witness is located. Similarly, accessing data located in another country, for instance on a cloud, can be difficult without the consent of the host country. The Budapest Convention and its Additional Protocol attempt to address such situations, but many complexities remain unresolved. The UN Convention on Cybercrime strengthened international cooperation, but did not introduce mechanisms to allow a state to directly order a company located in another state to provide data. This reaffirms the traditional principle of state sovereignty.

In conclusion, international law in the cyber context remains rooted in the traditional principles of sovereignty and consent. However, the practice of states will continue to evolve, addressing the challenges posed by technology.

THE DIFFERENT SETTINGS ON THE DEFINITION AND ATTRIBUTES OF VIRTUAL SPACE. THEIR CONSEQUENCES ON THE EXERCISE OF SOVEREIGN POWERS AND JUDICIAL COOPERATION

Dennis Wilder

Former senior US intelligence officer - Professor at Georgetown University's School of Foreign Service - Member of the National Committee on US-China Relations

As you probably understand, the United States is under siege by China, Russia, and others in cyberspace, with artificial intelligence a major component of these malicious attacks. As US Deputy Attorney General, Lisa Monaco, has often stated, the 115,000 women and men of the US Department of Justice are committed to proactive cyber strategy that prioritizes near-term disruptions and victim protection, while tackling the broader ecosystem that supports cybercriminals, including the abuse of crypto-currencies and disruptive technologies. As she has said, the United States has a "prevention-focused, disruption-focused, victim-centered" action plan. I will not delineate all the various initiatives at the Department of Justice, as you can find them on your own. Instead, let me talk about the sheer audaciousness of some of the attacks from China and Russia.

China-based hacking organizations, such as Volt Typhoon, Flax Typhoon, and Salt Typhoon, have successfully infiltrated the IT networks of the United States' critical infrastructure systems and United States Internet service providers (ISPs). According to the Office of the Director of National Intelligence's 2024 Annual Threat Assessment, these kinds of infiltrations are for wartime use by China in military conflicts to damage the United States' ability to use the resources provided by its critical infrastructure, which would slow down the formulation of appropriate United States military strategies.10

- According to the Cyber Security and Infrastructure Security Agency (CISA), Volt Typhoon successfully compromised the IT networks of communications, energy, transportation, water, and wastewater facilities within the continental United States and its territories, including Guam.[11]

10 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf
11 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

- According to a Department of Justice press release of September 18th, the Federal Bureau of Investigation successfully disrupted a botnet organized by Flax Typhoon that contained 200,000 devices and had successfully compromised United States corporations, government agencies, and telecommunications providers.[12]
- On September 26th, the Wall Street Journal reported that Salt Typhoon had broken into the networks of United States ISPs. If hackers had gained access to the core routers of the ISPs, they would have been able to access sensitive information and the personal data of American citizens.[13]

The targets and infiltration techniques of these hacking groups are significantly different from Chinese hackers' traditional patterns of cyber espionage, according to the CISA.[14] Unlike traditional Chinese cyber espionage, which has targeted companies' intellectual property using quick cyberattacks, these new cyber operations prioritize non-detection and longevity to successfully embed themselves and remain dormant within infrastructure systems' servers for an extended period.

- According to Microsoft, Volt Typhoon uses a variety of countermeasures to make detecting its activities difficult, including using legitimate credentials of individuals registered in the directory of critical infrastructure IT networks.[15] Microsoft also said that Flax Typhoon used similar tactics to remain undetected for as long as possible.[16]
- Multiple sources, including Microsoft and CISA, have stated that these Chinese-backed hacking organizations prioritize the longevity of their infiltrations and frequently check to ensure they still have access to compromised systems over time. This allows them to hide in IT networks for years while waiting to cause damage to their targets.[17]
- According to General Timothy Haugh, Director of the National Se-

---

12 https://www.justice.gov/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

13 https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835

14 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

15 https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

16 https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/

17 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

curity Agency, the presence of the Chinese state-backed hackers in the IT networks of critical infrastructure, which offer little value for collecting intelligence, is concerning because it suggests that China is positioning cyber assets to strike and disrupt critical infrastructure in the event that a military conflict occurs between the United States and China.[18]

Using hackers to disrupt the ability of critical infrastructure to function correctly would allow the Chinese military to gain an early advantage in future military conflicts with the United States. If cyberattacks made critical infrastructure such as communication systems unusable, before the United States could focus on creating a military strategy, it would need to restore these systems to enable coordination between military units and supply lines. Therefore, it is likely that the Chinese government will use hackers to attack the critical infrastructure of the United States in the early stages of a future military conflict between the two countries.

- Moreover, it is very likely that some Chinese-backed hacking groups have remained undetected and continue to threaten the safety and function of the United States' critical infrastructure. Surprise attacks from unknown organizations embedded in critical infrastructure networks would cause significant damage and be difficult for the United States to defend against.
- If Chinese hacking groups target civilian and military infrastructure, disruptions of resources like water and electricity would not only slow down effective responses from the United States military during a conflict but also harm United States civilian populations. If Chinese hackers can keep essential resources cut off for an extended time, it would likely amplify the suffering of the American people.

This kind of brazen cyberattack has many implications. The first is that these attacks do not discriminate between US and foreign companies. Anyone involved in US infrastructure is fair game as far as the Chinese hackers are concerned.

The second implication is that, while the US may be the first target, it will not be the only target of these kinds of attacks. In the context of the Taiwan Strait standoff, Beijing will not only want to degrade US infrastructure but those of US allies and partners who also come to the defense of Taiwan. Thus, we can assume that Beijing is already planning similar programs against not only Taiwan but such US allies as Japan, the Philippines, Australia, and the UK.

---

18 https://www.wsj.com/politics/national-security/china-is-prepositioning-for-future-cyberattack-sand-thenew-nsa-chief-is-worried-5ede04ef?mod=article_inline

The third implication is that it is inevitable that China's actions will lead the United States and its closest allies to explore the development of their own offensive capabilities against Chinese energy and other infrastructure. What China is doing will inevitably lead to an escalating cyber arms race in which both sides try to position themselves to use cyber space as a realm of warfare that is a force multiplier. Turning to another element of AI assisted cyber-attacks, the United States is experiencing the highest level of foreign malicious influence campaigns in the current Presidential campaign cycle that we have ever seen.

On 4 September, the Department of Justice announced that state-sponsored Russian hackers given a company called the "Social Design Agency" $10 million to generate, using artificial intelligence, content on the internet designed to undermine the American public's faith in the democratic process. Putin's agents also used unwitting US influencers to again create malicious content.

Iran's interference has been even bolder. Three Iranian hackers have for several years launched malicious attack of current and former US government officials and US journalists. They recently sent unsolicited emails to the Biden campaign containing non-public information stolen from the Trump campaign to undermine Donald Trump's run for the Presidency.

China's approach to malicious influence campaigns has been more subtle. Garphika has identified 15 accounts on "X" or Twitter that mimic US nationals and advocacy groups that call into question the legitimacy of the US elections. One of these posts had had 1.5 million views.

The final question I would like to wrestle with is: why are the Chinese and the Russians so bold?

An Extreme Paranoid

I believe that Chinese leader Xi Jinping often acts the way he does on such things as malicious cyber because of extreme paranoia of the United States and its allies.

- Xi has often referred to the "black hand" of the CIA in fomenting unrest in Hong Kong and he believes that the color revolutions have been the work of the West. During a private talk with President Obama, he said that China had been a target of "color revolutions," foreshadowing his obsession with national security.[19] [20]

---

19 Remarks by President Obama and President Xi Jinping in Joint Press Conference | whitehouse.gov (archives.gov)

20 GT Investigates: US wages global color revolutions to topple govts for the sake of American control - Global Times

- Most revealing were his remarks on the margin of the National People's Congress in March 2023 where he stated, "Western countries, led by the United States, have implemented all-round containment and suppression of China, which has brought unprecedented severe challenges to the country's development".[21]

Xi's paranoia extends even to his erstwhile friends. Today, former Vice President Wang Qishan, who was instrumental in Xi's anticorruption campaign, is not allowed to meet with foreign visitors. Similarly, former economic guru Liu He, who Xi had been friends with since grade school, has disappeared and the rumor is that he has been accused of corruption because of the business activities of his son.

Xi's paranoia has almost certainly been reinforced by the saga of former Foreign Minister Qin Gang. Qin Gang's paramour Hong Kong reporter Fu Xiaotian is believed to have been a spy for a Western power. Qin Gang appears to have convinced the leadership that he was simply a victim of a honey trap and that he never betrayed Xi or China. Whatever the truth, Xi apparently has decided it is in his own best interest to simply demote Qin Gang to an ordinary party member.[22]

As Xi ages, his paranoid tendencies are likely to be accentuated. Xi has apparently decided not to appoint a successor in order that he can remain China's leader for life. He has attacked successful leaders in China's emerging technology industry, such as Jack Ma, because he sees them as a potential alternate power center and threat to his authority.[23] His obsession with national security has led him to greatly expand the writ of the Ministry of State Security and the MSS has become increasingly bold in approaching Western businesspersons in China and warning them against anti-regime activities.

China Wants a New World Order

A second aspect of Chinese thought on the malicious use of cyber is that they want to reshape the international order to reflect their values. strife. In late 2017, Xi began to talk about "changes not seen in 100 years." The implication was that the United States, like the British and French Empires of the 1920s, was in long-term decline, while China was on a trajectory to become the world's most powerful nation by mid-century. At the end of his summit meeting with President Putin in Moscow in March 2023, Xi Jinping

---

21 China accuses U.S. of containment and warns of potential conflict: NPR

22 Ex-Chinese FM Qin Gang loses seat at party top table but may escape punishment | South China Morning Post (scmp.com)

23 The vanishing billionaire: how Jack Ma fell foul of Xi Jinping (ft.com)

was heard saying, "Right now there are changes—the likes of which we have not seen for 100 years—and we are the ones driving these changes together." The Russian president responded: "I agree."

The narrative of a West in decline and an East rising is open to challenge, especially now that China is struggling to regain economic momentum and Russia is bogged down in a seemingly unwinnable war in Ukraine. Nevertheless, the narrative of declining United States power ultimately serves Xi's purpose. It fits well with his "China Dream" of a rejuvenated great power dominating world affair by 2049, the 100th anniversary of the founding of the People's Republic of China.

The starting point for understanding Xi's vision is his Global Security Initiative. The GSI is founded on Beijing's dislike of the US-led international order, reflecting an ideological competition between the two countries. At the 20th Party Congress last year, Xi Jinping not so subtly differentiated Chinese foreign policy from what he characterized as the US foreign policy by declaring, "We have comprehensively promoted major-country diplomacy with Chinese characteristics ... and unswervingly opposed any unilateralism, protectionism, and bullying. We have promoted the construction of a new type of international relations, and actively participated in the reform and construction of the global governance system".

The Chinese authorities see this Western order as granting China privileges and membership in the privileged "club" only if China behaves according to Western norms and values. They believe that Washington uses its power and alliances to restrict China's development, including the Biden administration's sanctioning of over 300 Chinese companies for violations of US laws and restrictions on transferring technologies in artificial intelligence and quantum to China. This treatment convinces them that the United States will never treat China as an equal because Washington is determined to keep China weak and remain the world's pre-eminent power.

So, from Xi Jinping's point of view malicious action against the United States and the West in cyberspace is simply an extension of the "no holes barred" struggle he believes that he is must win in order for Chinese Communism to survive.

IMPLICATIONS ON INTERNATIONAL CRIMINAL JURISDICTIONS OF OPERATIONS IN VIRTUAL SPACE

Rosario Aitala
Judge - First Vice President of the International Criminal Court - The Hague

I will move onto somewhat different ground from what has been addressed so far, which is that of the international order in the proper sense. The international legal system regulates mainly a world of states, but in the field I deal with on a daily basis it also has repercussions on the activities of individuals, of subjects.

I have a caveat. I am going to talk about a number of topics that abstractly can relate to various conflicts going on in various parts of the world; of course I am not going to refer to any of them, I could not do so because I chair the preliminary section of the International Criminal Court, so I deal with them professionally and I am bound to secrecy. Some operations carried out in virtual space in the proper sense or conducted through electronic tools, automatic tools, machines and algorithms, may qualify as international crimes. They may therefore entail consequences in the international legal system as such. International jurisdictions, in particular the International Criminal Court, has jurisdiction over international crimes that protect very high interests: peace, international security, fundamental in a systematic sense of the world's populations, war crimes, crimes against humanity, genocide and aggression.

I will present three or four macro-themes, but I can only outline them, somewhat indicating a map of the problems that I can naturally neither address nor solve. I will take the first one off the table immediately, because it has also been addressed at various times by President Guerini, that of the use of cybernetic methods to commit attacks, acts of sabotage, and attacks on critical infrastructures. These acts can qualify as acts of terrorism, as war crimes, crimes against humanity, depending on the different circumstances. It is an apparently quite obvious subject, but there are no jurisprudential applications, practical applications; I think President Guerini has covered it quite adequately.

The second issue, which is more complex and very topical, is the use, as a method, as a mode of warfare, or as a mode of government control of populations, of machine learning systems, systems that are normally called Artificial, but are actually Intelligence Machine Learning systems, that is,

they are systems that work through algorithms that are taught what to do. They are given a set of parameters and then offered a set of data; these systems analyse it and use it at a speed that is absolutely unimaginable for any human being.

A first application, which is not recent, it has been used for many years now, is that of automatic weapons systems. These are weapons that, once they are launched, have discretion, so to speak; they can decide in real time what to do, identify targets, adapt to their surroundings and launch attacks on certain targets without any human intervention. They therefore make their own decisions, once activated. The legal, but also ethical, problem they entail is that, if are not takenadequate measures , human control falls away, and while one of the pillars of international humanitarian law in the law of armed conflict is the precautionary principle, which obliges states to take precautions so as not to strike at subjects extraneous to the hostilities, civilians or military personnel out of combat and civilian objects.

This issue has been debated for some time now and has been temporarily resolved through the criterion of *meaningful human control*, i.e. it is required that human control should remain in place, so that the machine, especially the drone, does not decide to target certain individuals because they look like militia but are not, or certain buildings that look like military buildings but are not.

From a jurisdictional point of view, this can have a number of consequences with respect to who decides the policy on the use of the instrument, who operates it and who has programmed it. Secondly, there are systems called DSS, in English Decision Support Systems, decision support systems for the conduct of war operations. How do they work? The algorithm accumulates a range of information: it is intelligence information, telephone data, biographical data, gender, age, place of residence, circle of friendships, social media acquaintances and so on. They then compile lists of targets to be hit militarily. They are accelerators, they do a job that intelligence agencies used to do together with the armed forces and military agencies, but they do it with extraordinary speed. One example: the head of the army of a major country, whom I do not want to name, explained the meaning of this in an interview last year. He says: we used to produce 50 targets a year, the machine produces 100 targets a day, and 50 of them we hit.

What are the critical issues? Firstly, the hard answer is no, the machine does not make mistakes, unless there is a technical fault or it has itself been manipulated by a hostile actor or competitor. The machine does not make mistakes. The machine does its job, that is, it provides answers according to its own algorithm and programming methods. So what are the unexpected

events that occur? What are they due to? First, they are due to uncertainties inoculated into the system. The system, for example, can distinguish the image of a militiaman with a rifle from that of a child with a stick. Yes or no? If it cannot distinguish it, it can kill a child; it is potentially a war crime. Second, it distinguishes colours, the position of objects. Global positioning systems (GPS) are inaccurate: a slight difference can lead to an attack on a hospital instead of a barracks, or on a kindergarten meeting of children instead of a militia training centre.

Secondly, *assumptions*: the system makes assumptions that have been taught to it by the programmer. For example, if an object comes towards my direction above this speed, it is an attack against us. Above 300 knots, it is an attack against us. These presumptions are sometimes wrong, particularly when they involve human beings, because these systems, in various conflicts, are taught to establish a degree, a *ranking of* dangerousness, or of characteristics that are those of the enemy, based on a series of elements. For example, I often change my mobile phone for professional reasons; it is an indication that I am a militiaman. All of us who have experience in investigating organised crime know that this is a mode that has existed for 35 years, since I started working; it is an indication. The other is the man: women are generally excluded. Another, the age: if he is over 60, he is probably not a militiaman; if he is younger, he may be. What is his circle of friends? Have you worked with someone who is close to that group? Yes or no? Is there anyone in his telephone contacts who is a military, an intelligence agent, an enemy militiaman? Yes or no?

On the basis of these presumptions it is carried out and, if I, unfortunately, get into these conditions but I am absolutely not a militiaman, I am not a military man, I am not an intelligence agent, I can be hit. Again, the responsibility lies not with the machine but with those who programmed it. Third, the system has biases, prejudices (biases) and preconceptions. These are also instilled by the programmer. One bias may be that of gender: he is a man; it may be that of being born in a certain area. I am Sicilian, I am from Catania, I was born in an area of high mafia density, it can be a *bias* whereby I actually gain a point or lose a point in the *ranking*.

One difficulty, therefore, is that of scheduling. Another is that of the time the operator has to accept the system's proposal. According to unverifiable, but nevertheless verifiable, journalistic investigations, in many of these cases the time available to the operator is only a few seconds, sometimes a few minutes. In that time, the operator is normally unable to assess whether the system has operated correctly, i.e. whether the target whose elimination he has accepted is a civilian, is a military, is a civilian object, a house, a hospital, a school, a university. Yes or no?

All these questions lead to a number of legal consequences. Firstly, what crimes can be envisaged? Various war crimes: intentional attacks against civilian property or persons or attacks such as to cause so-called incidental, collateral damage. And these are two of the crimes that come to mind.

The third determinant is the so-called "policy for casualties". What is the acceptable rate of casualties? That is, how many innocents can my enemy take to his grave? 1, 2, 10, 100? With this indication, the scenario changes radically, because the law of armed conflict revolves around three principles.

The first, that of distinction, requires us to distinguish between subjects against whom armed force can be legitimately used and subjects against whom it cannot.. And these are essentially the principles of the Geneva Conventions: civilians and combatants out of combat, who are no longer capable of armed activity., requires a to made be

The second principle is one of proportionality: the attack must be such, with a prognosis ex ante, in concrete terms, hence with an assessment that is made by putting oneself in the shoes of the decision-maker at the time of the decision, so as not to cause accidental damage disproportionate to the military advantage. Of course, in the case of protracted conflicts, or protracted situations, what has happened in previous cases has significance, because I already know what is going on, or, for example, with respect to conflicts that take place in urban environments, where it is much more difficult to distinguish.

The fundamental principle, however, is the precautionary principle: they must for these two reasons adopt ways to avoid accidental damage. And it is a process that must tend towards zero, must tend towards zero incidental damage.

Another fundamental point to bear in mind is that the possible violation of international law by the enemy does not legitimise a violation by the other belligerent: as if to say, opposing immoralities, opposing illegalities do not compensate, they add up.

Another example, and then I'll move on to the conclusion: there are systems also based on algorithms, on artificial intelligence, which allow mass surveillance. They are used in various autocracies, but not only, and they allow, on the basis of biometric data, of the iris, of the shape of the face, even of the way one moves, to control the movements of masses of people, even millions of people, and possibly to prevent these people from going to certain places, or to certain parts of a city, or in certain cities.

These can be, if they are based on arbitrary criteria, crimes against humanity of persecution on ethnic, religious, political or even apartheid grounds, i.e. within regimes that arbitrarily distinguish people on the basis of personal characteristics.

The last example, and I go to the conclusion that I only touch upon incidentally, is that of the use, also by cybernetic means, of everyday objects as instruments of war. Typically, the mobile phone, which goes with us all the time. If the mobile phone is used physically, or through cyber systems in such a way as to become, for example, an explosive object, this is a prohibited mode of warfare, because there is an international protocol that has been ratified by a great many states that prohibits the use of these traps, called in English *booby traps*.

To conclude. The tumultuous and unstoppable development, especially in the very last few years, of technologies that reduce the space of human control and increase the ways in which people's lives are controlled, brings with it a number of legal, ethical and political challenges. In the area I am dealing with, and which I am dealing with, there is no problem of non-regulation. International law exists, there are norms, it is the norms of international human rights law that protect fundamental rights, and the norms of international humanitarian law that regulate the legitimate ways and means of armed conflict and the actors who can be legitimate recipients of armed violence.

Therefore, the rules exist, there is no regulatory vacuum. However, as Prefect Guidi mentioned earlier, going back to Kelsen, the implementation of international law is of course left to states, because international law operates in this world of states, it is created by states, and states, fortunately, cannot easily change or destroy it through the use of custom to which Giovanni Salvi referred earlier. But they can, by their conduct, either strengthen the rules of law or empty them of meaning.

The subject is essentially political, because rules are legal rules, but also moral rules. The Pope, a few days ago, answering a question, said something very apt: "War is always immoral, but there is a certain morality even in war". The morality is the rules of international humanitarian law.

In recent days, in recent months, in recent years, we hear that the way conflicts or situations of persecution and within states have been going on in recent years indicate a flaw, an error, a failure of international law. I think this approach is wrong. The law is there, the rules are there, the failure is a political failure. It is states that must implement international law. Law and politics stand and fall together, but if international law falls, politics falls, and above all, the duty of politics falls, which is to settle disputes peacefully and, when necessary, to conduct armed actions within the tracks established by law and, above all, to limit that tendency to the extreme that was theorised by Clausewitz in a passage before the famous one of political war as another means.

Clausewitz said that war tends to the extreme, because the belligerents give each other challenges that raise the bar to the point of meeting the duty

of politics. And that, I believe, is the fundamental theme. And it is one of the reasons why this meeting is particularly important and why we, with few means, modestly and realising that we are only one link in a very complex system, have a duty to act as referees, to blow the whistle when there are infringements and, therefore, to point out when international law, especially that which concerns human beings, is violated.

SECOND SESSION

CYBERSPACE. THE UNITED NATIONS OPEN WORKING GROUP. THE UN CONVENTION ON COMPUTER CRIME IN JUDICIAL COOPERATION

CYBERSPACE. THE UNITED NATIONS OPEN WORKING GROUP. THE UN CONVENTION ON COMPUTER CRIME IN JUDICIAL COOPERATION

INSTITUTIONAL GREETINGS

Antonio Tajani

Vice-President of the Council of Ministers and Minister of Foreign Affairs and International Cooperation

I am delighted to host this important event at the Ministry of Foreign Affairs, which offers the opportunity to explore the challenges of virtual space. I greet the Vittorio Occorsio Foundation and all participants.

The challenges of the cyber world now have tangible consequences on the real world, which is why it is increasingly imperative to share every effort to counter threats. Teaming up is crucial. The government is at the forefront of the issue of security, which we have made a priority in Europe and in the G7. We have taken numerous measures to address the issue across the board and strengthened international coordination in this strategic area.

I also wanted to set up a Security Technology Innovation Unit at the Foreign Ministry. At the meeting of the G7 foreign ministers that I chaired in Capri in April, we strongly affirmed the crucial importance of ensuring that artificial intelligence is reliable and in line with our ethical values, keeping people and human rights at the centre. This important challenge can be turned into a great opportunity for our societies and businesses, fostering growth.

The Holy Father's words at the G7 summit in Puglia are a perfect representation of this approach of ours, which also animates the bill adopted in April by the government and currently under discussion in Parliament. Crucial are the security implications, particularly on the issue of disinformation, which introduces a very sensitive variable within our societies, especially at a time when our values are at stake in the face of autocracies.

In this regard, I signed with US Secretary of State, Antony Blinken an important agreement with the, in Capri to strengthen cooperation with the United States in the fight against disinformation. Appointments like today's show how fruitful collaboration between diplomacy and the judiciary can be in order to affirm the exercise of jurisdiction and the protection of rights in virtual space.

Count on me, count on Antonio Tajani.

CHAIRPERSON

Stefano Mogini
Secretary General of the Court of Cassation

Good morning, everyone. Allow me to thank, first of all, the Occorsio Foundation for the invitation and for the richness of our work, especially for its ability to honour the civic example of Vittorio Occorsio, calling for high-level analyses on the most relevant issues for our societies, and for its ability to federate so many institutions at national, supranational and international level on these issues.

Let me also bear witness to the Foundation's ability to be present, to provide a special leaven where the minds and consciences of our country's young people are being formed. As were told yesterday by the representatives of the Foundation, it takes intelligence and courage. I still have in my eyes, for example, the initiatives carried out precisely at the Court of Cassation by the Occorsio Foundation with the participation of so many young people from schools, including that of the Technical Institute of Caivano, which was also present here yesterday to remind us of the importance of respect for legality, rules and commitment to the common good.

So, thank you to the Foundation for all this. I would also like to thank you for this opportunity to return to this house, the Farnesina, which has played such a large part in my professional and human career, during which I had the privilege of serving for several years at the Italian Embassy in Paris as liaison magistrate, and then for six years in New York at the Permanent Representation of Italy to the United Nations as *Legal Advisor*.

It is an administration, the Ministry of Foreign Affairs, from which I learned a lot and for which I have sincere gratitude and great admiration. I also bring the greetings of the First President of the Court of Cassation, Margherita Cassano, who is on a mission abroad but follows all the activities with great interest and closeness.

The Foundation's activities this morning will focus our attention on the efforts being made in the global international forum par excellence, the United Nations, to develop an international legal framework, a multilateral discipline of virtual space.

Our focus will be on the adoption of the UN Convention on Cybercrimes. To do this, we can count on top-level experts who have been protag-

onists in these efforts, in important roles and representing national positions or groups that do not always coincide.

It will be interesting to hear their assessment of both the negotiation processes and the results these negotiation processes have produced or what they hope to achieve in future work.

WORKS AND POTENTIAL DEVELOPMENTS OF THE UNITED NATIONS OEWG ON THE DISCIPLINE OF VIRTUAL SPACE

Michele Giacomelli
Special Envoy of the Ministry of Foreign Affairs and International Cooperation for Cybersecurity

I want to begin by extending my heartfelt thanks to the Fondazione Vittorio Occorsio. I have been asked to speak about "Works and potential developments of the UN OEWG on the discipline of virtual space. It is a subject that I am pleased to explore with you as it is extremely timing.

The Chair of the OEWG has just introduced a draft Resolution in the First Committee for approval of the third Annual Progress report approved in the July session.

I believe it is important to start with a brief historical overview of how the norms and rules governing this domain have evolved from the end of last century - when it appeared that the rapid proliferation of information and communication technologies (ICTs) brought the necessity of global cyber regulations, as these technologies increasingly posed new threats to international security – to today.

The creation of the UN Group of Governmental Experts (UNGGE) dates back to 2004. While the initial progress was limited, the group's membership gradually expanded from its original 15 states, and three key reports were produced in 2010, 2013, and 2015. In 2018, following an initiative spearheaded by the Russian Federation, the UN General Assembly established by Resolution the OEWG (Open Ended Working Group on security of and in the use of information and communications technologies) with the goal of involving the broader UN membership, particularly developing countries, in addressing cyber issues.

The OEWG published its first report in 2021, and its mandate was subsequently extended for five more years (2021-2025), with the current term set to expire next year. There is an ongoing debate on how to continue the regular institutional dialogue, either renewing the OEWG's mandate or replacing it with a Program of Action (PoA), as many Western states have advocated, in an effort to make the group's efforts more action-oriented, open to multi-stakeholders' contribution and capable of addressing different themes in a cross-cutting way. At the heart of these discussions are longstanding challenges: diverging views on the ways to ensure the responsible state behavior

of States in cyberspace, and differing interpretations of how international law applies to this domain, which NATO refers to as the "fifth domain," in addition to land, air, sea, and space.

There is a clear divide between Western states (the EU and like-minded) and a small number of other states, led by the Russian Federation. The large group of States composing the so-called middle ground tend not to take side. They may offer constructive proposals (such as Brazil's call for a moratorium on First Committee Resolutions or India's proposal for a Portal to coordinate cyber capacity-building efforts).

Western states, broadly speaking, believe that the current normative framework is adequate to regulate cyberspace and prevent conflict. They argue that the existing international legal framework is sufficient, with no major gaps. The fundamental position is that cyberspace is not lawless. The laws and norms that govern other domains can and should be applied to regulate cyberspace as well. While the possibility of creating new norms is not entirely ruled out, such steps should only be considered after a thorough review and assessment of existing gaps and interpretive differences.

Conversely, a significant number of states maintain that cyberspace is unique and that norms created for other contexts cannot simply be transposed. For this reason, they call for the creation of a legally binding convention specifically tailored to the cyber domain. This remains a key point of divergence.

Many fear, as several observers and researchers have noted, that the call for new regulations may be a strategy to evade the current framework. There is concern that such a convention could weaken existing restrictions, particularly regarding non-state actors, who are often responsible for malicious activities. In truth, this debate is political as well as legal.

What are the components of the aforementioned framework?

It consists of a combination of general, treaty-based, and customary binding norms, borrowed from the kinetic world and applied by analogy to cyberspace. Complementing these are the 11 voluntary, non-binding norms adopted in 2015 by the UNGGE on Responsible State Behavior. It is now widely accepted that the UN Charter and the principles of international law apply to cyberspace. The point of contention is not whether international law applies to cyberspace, but how it applies.

Several key principles are central to this debate, including:

- State sovereignty, which can be violated even without the illegal use of force;
- Non-intervention, where the unauthorized use of ICT systems within a state's territory can be deemed an illegal intervention if the scope and effects are comparable to those of non-cyber interventions;

- Use of force, the threat or use of force against the territorial integrity and independence of another State, as outlined in Article 2(4) of the U.N. Charter, hinges on the concept of a threshold, beyond which the use of force is deemed to have occurred. In this context, the most reliable measure appears to be the effects of the force used - specifically, whether the scale and impact of a cyberattack, either ongoing or threatened, are comparable to those of a kinetic military action.
- The right to self-defense, which involves assessing whether the threshold of an armed attack, as defined in Article 51 of the UN Charter, has been crossed, and consequently, whether the response is proportionate and necessary;
- State Responsibility, is an extremely sensitive issue, as it involves the process of attribution. In practice, it is necessary to establish the state's responsibility clearly and conclusively. In today's world, this is not easy. Malicious activities are primarily carried out by non-state actors, whose granular nature makes it challenging to definitively link them to a specific state. This is why the attribution process is so complex. It is common to distinguish between technical attribution and political attribution to highlight the process's complexity and to emphasize that, ultimately, the decision to attribute malicious activities to a state always falls within the sovereign competence of another state and is primarily driven by political considerations. Due to this complexity, a precise threshold for when cyber activity constitutes the use of force has not been defined yet. Public attributions of responsibility, as we have seen in recent times, are often rejected by the accused states as politically motivated and not based on compelling evidence. While the international community widely condemns malicious behaviors, particularly those targeting critical infrastructures or sensitive sectors such as healthcare and energy, there must also be a pragmatic understanding of what tangible results can realistically be expected just from a name and blame exercise.
- Countermeasures, these depend on identifying the responsibility of the aggressor state. They are subject to the same limitations in the cyber world as in the non-cyber world, including proportionality, obtaining reparations, and transparency;
- Due diligence: States are obligated to ensure that their territory is not knowingly used to conduct cyber activities that infringe upon the rights of other states. The general principle of due diligence also implies that reasonable preventive measures must be taken, which may require each state to have a minimum level of ICT infrastruc-

ture and governance capabilities. Essentially, this is an obligation of conduct, not necessarily of result;

- Peaceful settlement of disputes: this principle extends to disputes involving cyber activities between states;
- Respect for human rights, according to the prevailing interpretation, international human rights law applies to cyber activities in the same way it applies outside the cyber context—both online and offline. Citizens are entitled to the same rights, and states are obliged to ensure respect for human rights;
- International Humanitarian Law (IHL), it is generally accepted that, in cases of armed conflict, IHL applies to the cyber domain. However, during the latest OEWG session, Russia and other states opposed the explicit mention of IHL in the text..

Scenario-based simulations, built around hypothetical incidents and responses, organized by international organizations like UNIDIR or research institutes, have proven useful in fostering mutual understanding. Equally important are the national positions on the application of international law that a few states (though not many) have published in recent years. Italy, for instance, conducted such an in-depth study in September 2021, thanks to a collaboration between the MFA, the Presidency of the Council of Ministers and the Ministry of Defence. The EU has prepared a common position which should complement, not substitute, the national positions.

In this milieu, I would also like to mention the Tallinn Manual, an academic document first published in 2013 by Cambridge University, following an initiative of the NATO Cooperative Cyber Defence Centre of Excellence. Initially, the text focused primarily on jus ad bellum situations, typical in the context of armed conflict. In 2017, an updated version of the manual was published, expanding its scope to cover the norms of international law that govern the cyber incidents states encounter. The Tallinn Manual, along with similar publications, serves as an authoritative reference for interpreting international law in cyberspace.

Thus far, we have discussed general treaty and customary norms. Complementing these are the 11 non-binding norms on responsible state behavior, another essential element of the framework. These norms provide guidelines to direct state actions and assess their compliance. Three of the norms concern prohibitions on what states must not do: they must not allow malicious activities to be conducted from their territory, they must not harm critical infrastructure, and they must not damage emergency response teams. On the other hand, the remaining eight norms focus on positive actions: states must work to foster cooperation and respond to requests for assistance. Are these

norms exhaustive, or are they subject to evolution? The OEWG Chair's synthesis at the July 2024 session was that both paths should continue. I quote from the Annual Progress Report (APR) "the OEWG must, acting on a consensus basis continue, as a priority, to further develop the rules, norms, and principles of responsible behavior of States and the ways for their implementation, and, if necessary, to introduce changes to them or elaborate additional rules of behavior." To promote greater convergence the Chair, supported by Member States, developed a Voluntary Checklist of practical actions (for the implementation of the norms of responsible state behavior in the use of ICTs). This Checklist is considered a living document, meaning it is intended to evolve over time.

But real questions remain: are these 11 voluntary norms being applied or not? And if they are not, why? What mechanisms are in place to encourage states to implement them? The international community still has a long way to go in finding definitive answers to these questions.

Alongside these central issues, the OEWG's mandate also encompasses several interconnected topics, which include:

- Identifying both new and traditional threats: while conventional risks to critical infrastructure remain a priority, we are now also confronting emerging challenges such as ransomware, AI applications, cryptocurrencies, and quantum technology.
- Confidence-Building Measures (CBMs): these are essential to prevent states from being caught off guard or misinterpreting each other's actions. In March 2024, the UN launched a new PoCs Directory (the register of points of contact within the UN) a voluntary tool designed to enhance communication and cooperation, building on similar efforts by the OSCE. In this area, regional organizations play

a significant role, such as the OSCE, which has approved 16 CBMs (Italy sponsored the number 14, on public-private partnerships).

- Cyber Capacity Building (CCB): this initiative aims to help states strengthen their political and technical resilience, enabling them to defend against and respond effectively to cyber threats. Recent discussions have centered on the creation of a UN portal to aggregate all capacity-building initiatives and the potential establishment of a dedicated CCB fund, possibly open to private contributions.
- Institutional Dialogue: in addition to the OEWG vs. PoA debate, the issue also involves the inclusion of non-state stakeholders and, consequently, the relationship with the private sector (Russia and China seek to limit this and emphasize the intergovernmental nature of the process).

Conclusion

In conclusion, the regulation of cyberspace is deeply influenced by the broader geopolitical context. As a result, the debate is marked by significant polarization. The division between creating a new convention and implementing existing norms, as well as between an intergovernmental approach and a multistakeholder model, reflects a fundamental lack of mutual trust and divergent worldviews.

Of course, dialogue and discussion are essential, but finding common ground remains challenging. This has been evident in recent negotiations within the UN on the Cybercrime Convention and for the finalization of the Global Digital Compact, which was adopted during the ministerial segment of the UN General Assembly in recent weeks, along with the Pact for the Future.

Nevertheless, if we have a perspective of decades more than years we may argue that progresses are possible. Ultimately, the path to multilateralism is never straightforward, and cyberspace is no exception. We must continue to engage with these critical issues, leveraging diverse perspectives and expertise. It is crucial to involve a wide range of professionals and stakeholders in this ongoing dialogue.

HOW TO MAKE MULTILATERAL JUDICIAL COOPERATION ON CYBERCRIME EFFECTIVE: A MULTIFACETED PERSPECTIVE ON CYBERSPACE

Eric Do Val Lacerda Sogocio

Vice-Chair of the Ad Hoc Committee for the Elaborate of an International Convention on Cybercrime. Former Head of the Division against Transnational Crime, Advisor to the Ministry of Foreign Affairs of Brazil

I would like to first thank the Vittorio Occorsio Foundation and the Presidency of the Council of Ministers for inviting me here today. As I mentioned to Mr. Giovanni Salvi during our preparations for this conference, it is an honor to see my name listed among such an eminent group of practitioners and academics dealing with different aspects of cyberspace.

I am also thrilled to share this panel with Margherita Cassano, our Chair; Michele Giacomelli; Luigi Birritteri; Glen Prichard; Antonio Balsamo; and especially Ambassador Deborah McCarthy, an excellent partner over the past few years during the negotiations of the United Nations Convention Against Cybercrime. There is a rich history behind the convention's lengthy and intriguing title, and if time permits, we can delve into it during the debate.

Today, I propose to:

1. Discuss the issue of jurisdiction from the perspective of international cooperation in combating cybercrime, arguing that cybercrime should be addressed separately due to its unique characteristics.
2. Examine key aspects of the UN Convention and how it equips countries to strengthen resilience against international challenges, thereby enhancing national security and the safety of citizens.
3. Share insights into Brazil's approach to jurisdiction concerning the acquisition of evidence and relationships with service providers.

First, why should international cooperation in combating cybercrime be treated differently from other cyber issues like cybersecurity, cyber defense, or cyberspace governance?

In essence, national jurisdictions — or sovereignties — will only cooperate if they choose to. There is no mechanism to compel a country to cooperate against its will.

Consider an example from the "*Proposta di Evento Collaterale*" that guided this conference's preparation:

"A hacker attack on strategic structures can simultaneously constitute a crime, punishable under criminal law, and an aggression against national sovereignty. The latter can constitute a violation of International Law (IL) and International Humanitarian Law (IHL), the consequences and reactions to which are governed by the instruments of that body of norms." Suppose the affected country's authorities view the attack as a crime and aim to prosecute the perpetrators. They need a clearly defined crime, an identified suspect, admissible evidence, and a demonstrable link between the act and the individual. Intelligence alone isn't sufficient; hard evidence is often necessary, as is the case in Brazil's legal system. If the suspect resides in another jurisdiction, authorities must formally request assistance from that jurisdiction to obtain the necessary evidence. This cooperation typically relies on bilateral mutual legal assistance agreements, international conventions like the Palermo Convention or the Budapest Convention, or simple reciprocity. A critical factor here is double criminalization: countries will assist if the conduct is criminal in both jurisdictions. However, if the other country chooses not to cooperate, the process stalls. Any number of reasons—ranging from substantive legal grounds to procedural technicalities like document formatting—can justify refusal. Thus, international legal cooperation in prosecuting cybercrime hinges entirely on mutual willingness.

This challenge was evident during the negotiations of the UN Convention Against Cybercrime. The initial draft circulated by Russia conflated concepts by addressing defense, security, and crime within a single instrument. Countries like Brazil had reservations about this approach. Fortunately, as negotiations progressed, the focus narrowed to cybercrime, enabling adoption even in a challenging international climate.

Another misconception was that a multilateral convention could compel countries to cooperate. In reality, the convention provides shared definitions of crimes—satisfying the double criminalization requirement—and offers tools for cooperation to willing countries.

Cooperation involves engaging with counterparts, not opponents. It's about recognizing, not asserting, sovereignties. This aligns with the African philosophy of Ubuntu: "I am because you are." Therefore, combating cybercrime through international cooperation reinforces jurisdictions and sovereignties. This partnership-based approach sets cybercrime apart from other cyber domains. When sovereignties are in opposition, issues fall under cybersecurity or cyber defense, requiring different strategies like attribution and promoting responsible state behavior in cyberspace.

Second, the UN Convention provides a foundation for jurisdictions to criminalize specific acts and facilitates effective international cooperation.

The convention outlines cyber-dependent crimes that member states should enact domestically:

- Illegal access
- Illegal interception
- Interference with electronic data
- Interference with information and communication technology (ICT) systems
- Misuse of devices
- ICT-related forgery
- ICT-related theft or fraud

It also defines cyber-enabled crimes such as:

- Child sexual abuse materials
- Grooming for committing sexual offenses against a child
- Non-consensual dissemination of intimate images
- Laundering of criminal proceeds
- Participation and attempt in criminal activities

By adopting these definitions, countries meet the double criminalization requirement, enabling them to request and offer cooperation in investigations and prosecutions. Timely exchange of information and evidence is crucial, given how easily data can be altered or deleted in cyberspace. The convention addresses this through a 24/7 network in each member state for expeditious requests. Preservation of data is key, as is the ability to exchange electronic evidence for serious crimes—those warranting a maximum penalty of at least four years' imprisonment, per the Palermo Convention. Combating cybercrime necessitates partners, not adversaries. Jurisdictions benefit when all counterparts—not just allies—can effectively perform their criminal justice functions. This underscores the importance of capacity building to prevent weak links in the chain.

By strengthening other countries' capacities, we reinforce sovereignty and the role of jurisdictions globally. The goal is universal minimum standards of criminalization to eliminate safe havens for cybercriminals. This further supports the argument that cybercrime should be addressed distinctly from other cyber areas.

Third, let's examine how Brazilian legislation handles jurisdiction in accessing information and evidence. The Brazilian Civil Framework Law on the Internet mandates that companies offering services in Brazil must comply with Brazilian legislation and court orders. This applies regardless of where the data is stored or where the company is headquartered. This approach reinforces national jurisdiction and sovereignty—not against other jurisdictions, but in favor of citizens and the national legal system. Accordingly, the Brazil-

ian judiciary requires companies operating in Brazil to maintain legal representatives within the country who can receive and process court orders and are liable for noncompliance. This hasn't been without opposition. A notable case involved Facebook (now Meta), which petitioned the Supreme Court to rule on the constitutionality of the legal cooperation agreement between Brazil and the United States. Their aim was to mandate that judicial requests follow the lengthy international mutual legal assistance process, rendering direct compliance with Brazilian court orders ineffective. Ultimately, the Supreme Court upheld the agreement's constitutionality but affirmed that companies must comply with Brazilian law and can be directly approached by Brazilian courts via their local representatives. Traditional bilateral cooperation remains an additional avenue, not the sole one.

In recent years, Brazilian courts have enforced compliance by temporarily blocking access to applications like WhatsApp and Telegram when they failed to respond to judicial requests or appoint legal representatives. Most recently, X (formerly Twitter) was suspended for 39 days until it complied with orders to remove accounts, appoint a legal representative, and pay fines for noncompliance.

Upon compliance, X stated:

"X is proud to return to Brazil. Giving tens of millions of Brazilians access to our indispensable platform was paramount throughout this entire process. We will continue to defend freedom of speech, within the boundaries of the law, everywhere we operate." The phrase "within the boundaries of the law" emphasizes the importance of adhering to each jurisdiction's legal framework, reaffirming jurisdiction to ensure citizens' safety and security.

However, we must be realistic. During the UN convention negotiations, many delegates noted that big tech companies often ignore their requests. A robust domestic legal framework, effective regulations, and significant influence may be necessary for countries to assert jurisdiction successfully.

In conclusion, returning to our panel's title—"How to Make Multilateral Judicial Cooperation in Cybercrime Effective: A Multifaceted Perspective on Cyberspace"—the UN Convention Against Cybercrime, as a multilateral legally binding treaty, empowers member states to assert their jurisdictions collaboratively in ways that would be less effective individually.

Deborah McCarthy

US Ambassador at the United Nations Ad Hoc Committee on cybercrime

Good morning, I am very honored and pleased to have been invited to this important discussion and I would like to thank the Vittorio Occorsio foundation and the Italian Ministry of Foreign Affairs and international cooperation. It is a personal pleasure to be back in Rome as I spent three and a half formative years in the beginning of my diplomatic career as the chief of staff to the us ambassador to Italy. I have had the pleasure of working with my Italian colleagues all over the world ever since, including most recently in successfully concluding a new cybercrime treaty at the united nations.

Today, I will first give an overview of our national cybersecurity strategy to put into context my subsequent comments on the new un cybercrime agreement. The us 2023 national cybersecurity strategy is built on five pillars which include:

1. defending critical infrastructure,
2. disrupting and dismantling threat actors,
3. shaping market forces to drive security and resilience,
4. investing in the future, and
5. forging international partnerships to pursue shared goals.

Each pillar stresses the need for collaboration across diverse communities, including the public sector, private industry, civil society, and international allies and partners.

This has been an important part of the us approach to the un cybercrime negotiations and will affect how we will monitor its' implementation. in our view, this collaboration is critical to effectively fight cybercrime.

But back to the overall strategy: it is important to note that the us made two fundamental changes domestically in how it allocates roles, responsibilities, and resources in cyberspace: the first was to shift the burden to defend cyberspace from the end user to the owners and operators of systems and the technology providers that build and service them. as an example, the president issued executive order 14028 in may 2021 which required service providers to share cyber incident and threat information that could impact government networks. the order also established baseline security standards for the development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available. The second change was to realign incentives to favor long term investments. the government has been working to change incentives to ensure that market forces and public programs alike reward security and resilience, embrace security and resilience by design and strategically

coordinate research. this has been done in part via presidential executive orders and memoranda which, among other things, set cybersecurity requirements in key sectors, as well as via legislation in congress such as the chips act.

For the purposes of our discussion on cybercrime today, i will note that pillar two of the strategy focuses on disrupting and dismantling threat actors. on the domestic side, this has led to tighter internal coordination by: 1) expanding the capacity of the national cyber investigative joint task force (NCI-JTF) which includes 30 us agencies, law enforcement and the dept of defense; 2) expanding public private mechanisms to share information including intelligence information and to work together to disrupt malicious operations; 3) focusing on ransomware including via a dedicated task force. of note is the underlying belief that service providers must make reasonable attempts to secure the use of their infrastructure against abuse or other criminal behavior.

Pillar 5 of the strategy focuses on international partnerships to pursue shared goals, multilaterally, regionally and bilaterally. new initiatives have included: the freedom online coalition, the quadrilateral security dialogue between the Us, Australia, India and Japan, the US-EUttc, the ransomware initiative. They include ongoing discussions for a US-EU agreement on access to electronic evidence in criminal proceedings. pillar 5 includes cooperative efforts to call out, attribute and punish state actors who violate agreed upon norms of responsible state behavior in cyberspace. it also calls for international efforts to secure supply chains. very importantly, it stresses the importance of strong coalitions to set norms and standards in various forums and to push back on efforts to expand state control over the internet in order to control the information space. In the wake of the rise of AI, I note that this pillar includes the us participation in the council of Europe's framework convention on artificial intelligence and human rights, democracy and the rule of law which sets a shared baseline for how we use ai . another example would be the recent us and like-minded sponsored un resolution to promote safe, secure and trustworthy artificial intelligence systems.

Lastly, pillar 5 includes robust efforts to provide expertise, training and assistance to countries via several us agencies. examples of this is the extensive ministry of justice work across the globe to provide digital evidence training and technical assistance to help collect and use electronic evidence. another different example is my very own ministry's new international technology security and innovation (ITSI) fund to support the development and adoption of secure semiconductor supply chains and telecommunications networks. I mention this because, as we think of international cooperative mechanisms to fight cybercrime, the role of capacity building, including legal as-

sistance to re-write laws, is critical. as we saw in the ahc negotiations, it was the desire for this assistance that pushed many countries to join consensus.

Having outlined how we approach cyber domestically and internationally, i would like to turn to the recently concluded new un cybercrime convention. It must be pointed out that when this process was launched back in 2017 by Russia, China and others, the aim was to have a non-Budapest convention. Many countries could or did not want to join Budapest. A Russian drafted resolution to begin discussion was tabled in 2019, which the us opposed. The resolution was adopted 88 to 59 with 34 abstentions.

Fast forward to the beginning of actual negotiations in January 2022. thanks to arduous work by our partners and like minded, we shifted the focus from the Russian draft to an alternate draft drawn from Budapest, UNTOC, UNCAC and a few regional agreements. The negotiations were tough and it was not clear there would be success. however, this past august, the draft convention was adopted by consensus. there was drama and controversy until the very end.

What was achieved?

1. a draft convention which, as i noted, has the bulk of its content drawn from existing international agreements like Budapest, UNTOC and UNCAC. that was a win, as, in the beginning, Russia and China had tabled their own text, which was very different and very broad, covering issues related to cybersecurity, information security and internet governance.
2. an agreement which has a narrow list of cybercrimes, listing only those which are cyber dependent, such as illegal access, illegal interception, interference with electronic data, that is, crimes that is did not exist before the advent of the internet plus a few important cyber enabled crimes covering money laundering and child sexual abuse / exploitation and online solicitation. we were able to successfully prevent the efforts of many countries to include another 20 vaguely defined so called "cybercrimes "which could have affected free speech and other liberties. however, these crimes are likely to be reproposed in discussions on a future protocol to the agreement which is provided for in the accompanying resolution.
3. An agreement which goes beyond existing international instruments for law enforcement in including human rights protections. this is the first time a un criminal justice convention has included an anti-discrimination grounds for refusal, for example. on an important note, this will also be the first un treaty which defines child as someone under 18 for purposes of offenses related to CSAM[24], which includes a robust and comprehensive definition of CSAM and which

24 CSAM is the acronym of Child Sexual Abuse Material (NDR)

calls for the criminalization of the broadcasting of CSAM, accessing CSAM online, possessing CSAM and grooming children online.
I note that the agreement also provides for the sharing of electronic evidence for investigations of serious crimes, with the definition of the latter coming from UNTOC. The safeguards and protections included in articles 6, 24 and 40(22) apply to these crimes. the aim here is to help assist in crimes for which there is electronic evidence, not just cybercrimes. I also note there is an article which covers the protection of personal data.

4. An agreement which during its three years of negotiations, led more countries to join Budapest, including Nigeria and Brazil.
5. And finally, an agreement which many of the small and middle ground countries agreed to join, as it offers them the possibility to adapt their laws and build their capacity to fight cybercrime. together with key partners, we repeatedly stated that we are ready to assist in this effort. What does the new agreement bring to us law enforcement? it will increase our reach in catching cybercriminals and add to pursue those who use cyber to sexually exploit children. among other elements, the new convention: a) automatically updates all our old extradition treaties to add cybercrime and online sexual offenses; b) ensures dual criminality for these offenses – all parties have to criminalize the same crimes. so, we can extradite from non-Budapest countries' and c) allows the us to ask for extradition from countries with which we have no agreement.

What are next steps? The instrument will be reviewed by two un committees before being submitted to the united nations general assembly for approval. it is expected to be approved by consensus. But the process will not end there. besides national signature and ratification, built into the accompanying resolution is the provision for discussions on a possible protocol beginning in 2026. These discussions will focus, inter alia, on additional crimes for possible consideration by the conference of parties for inclusion in the instrument. Though the threshold for adoption of any protocol is high (60) countries, there are risks of expansion into areas which we and our partners do not deem to be cybercrimes.

I would like to conclude by speaking a bit on the role of civil society, industry and others in fighting cybercrime. During the negotiations, in an unusual procedure, many stakeholders were present. they were able to offer comments, submit proposals and more. Though not all of their suggestions were included, we believe that stakeholders are an essential part of the process. Many, particularly the private sector, are often the primary victims of

cybercrime. Therefore, their input on how the new treaty is being implemented will be critical. the same can be said for the multiple human rights groups. They are very concerned about a new un instrument which includes countries such as Russia, China and others who have a very different definition of cybercrime and may seek to target their citizens overseas or to pressure weaker states to share information. We believe that going forward, we will need to have the stakeholders by our side in monitoring the implementation of the instrument and to call out any abuses by certain governments. in my explanation of position at the end of the negotiations, I emphasized that we would be vigilant and use various instruments of power, including sanctions in cases of abuse. I expect we will be restating this position again.

MULTILATERAL COOPERATION IN CYBERCRIMES BETWEEN NEW CONVENTION UN AND SECOND PROTOCOL BUDAPEST CONVENTION

Luigi Birritteri
Head of Department for Justice Affairs - Ministry of Justice

Thanks to the Occorsio Foundation for the repeated opportunities for in-depth study in which it is engaged. Thanks to the work of Giovanni Salvi in this particular and delicate matter. After what has been said by Eric Sogocio and the ambassador, I must make a criticism of the American system because I really do not understand how they can allow Ambassador McCarthy to retire before she is 99 years old, but apart from that, I will try to show you the other side of the moon, having participated in all the negotiations in New York, which were the most complex and painful ones.

And I say at once, the text of the Convention is a text of compromise, of strong compromise, gained on the ground thanks to the invaluable work of the chairwoman of the Commission Merbaki and the vice-chairman Eric Sogocio, who was an invaluable negotiator with the whole band of South American countries, Latin American , the United States, the Canadians, the Japanese, the whole bloc of Western countries that walled off a broad convention, one that did not take into account the principles of *Serious Crime*, one that was open to any type of crime committed.

So a compromise text was agreed, with safeguards won on the ground, our red lines, all of which were accepted, even after a vote that Iran repeatedly demanded, as Professor Milanovic mentioned. I am referring to Article 14, which I will perhaps tell you about later, on child pornography. It was a tough battle had, and this must be said with absolute clarity, that only one possible alternative: the failure of the negotiations, which was feared up to four days before the negotiations were unblocked.

Therefore, the principle of reality leads us all to say that we must also deal with countries that do not have the same model of Western democracies, we must negotiate in search of what can only be a compromise text. Ambassador McCarthy did well to recall that the initiative was taken by Russia and China, albeit in a very different geopolitical context. Above all, she was right to point out that from the were sought to be outset dozens and dozens of criminal offences included that had only one common thread, that of international cooperation aimed at repressing dissent inside and outside those countries, an

attack on human rights and Western democracies.

The game was therefore to choose a satisfactory compromise text between the requirements of judicial cooperation, MLAs, transfer of trials and whatever else has been brilliantly discussed so far, with particular regard to the need for digital evidence to be immediately captured, properly preserved and, if I may be permitted to quote from Giovanni Salvi's brilliant speech, also to pose the question of the genuineness of the evidence acquired, of the correctness of the electronic data acquired, which is the foundation for a to be born correct criminal investigation on the basis of data that is tested and controllable, as well as correctly stored, immediately blocked and rapidly exchanged.

But beyond that, there was the need to create a barrier for the respect of human rights. And when I speak of human rights, I am referring to that elaboration of doctrine that sees cyberspace not only as a frontier of criminal danger, but as an additional tool for organised crime circuits to carry out the most serious crimes that other UN conventions normally deal with, from the Palermo Convention to the Merida Convention, as Stefano Mogini has well quoted. This aspect of human rights will perhaps make it possible in a few years' time to elaborate that, among the fundamental human rights, the right to free access to the web, free access to cyberspace, the freedom to express opinions, which can legitimately be included in a new, broader notion of human rights, will also be included.

I am merely saying, without recalling the effort it cost to insert this rule, to recall Article 2, paragraph 2 of Article 6 of the Convention, which says precisely that no provision of this Convention shall be interpreted as allowing the suppression of human rights or fundamental freedoms, including the rights related to freedom of expression, conscience, opinion, religion, belief, peaceful assembly, and association, in conformity and in a manner consistent with applicable international human rights law. Those who took part in the negotiations know how much effort it took to insert this rule, together with Article 24, along with the other rules that are real barrier rules, which will make it possible to prevent cooperation when there is a suspicion that the request for judicial cooperation is not based on the need to prosecute a *Serious Crime*, as agreed in the text of the Convention in Articles 9 to 16, but is based on the need to repress internal political dissent.

We are well aware of this, just as we are well aware that the point of arrival of the Second Protocol of the Budapest Convention is a point of arrival with a strong western traction compared to which the enlargement that is necessary at the level of the United Nations, where there are 194 potential subscribing countries (if I am not mistaken, the count is 192, those that par-

ticipated directly in the negotiations), is a point of compromise that some, reading the specific rules of cooperation, as Giovanni Salvi, for example, has just pointed out, can read in a minimalist sense.

But the real game is to ensure a cooperation instrument that, in the wake of Budapest, can expand the possibility of cooperation, together with the need for *capacity building* for all those countries that are ill-equipped in the fight against cybercrime.

That said, wanting to pick up the thread of the speech I had prepared, I stress that the Convention addresses necessarily harmonised offences, not identical offences. The provision for cooperation in terms of double criminality is based on the factual case being prosecuted and not only on the title of the offence. Harmonisation means not expecting each participating state to have identical or photocopied criminal provisions, but merely describing cybercrimes on the basis of *Serious Crimes* as envisaged in the draft convention.

It will then be the study, the evolution, the ratification laws, i.e. the path after the approval phase, which should take place in November, in the individual member states that will explain to what extent this Convention will apply only to cybercrimes in the strict sense, i.e. those that are committed only through the web, or whether there is an instrumental link with reference to cybercrimes in the improper sense, i.e. ordinary crimes that can also be committed through the use of the web. The classic example given is fraud.

The Convention, then, seems to me to be appreciable in terms of guaranteeing the acquisition of electronic evidence in the process, which is all the more challenging in the context of *cloud computing*, a context in which data is distributed by multiple providers, in multiple countries, in multiple servers.

I believe that the fact of envisaging, as does the Convention Budapest, but in an even more pregnant manner than the latter, the collaboration of *server providers* in the phase of the acquisition of evidence is one of the most interesting parts of the draft, which will then have to see implementation in the individual laws of the Member States that will have to transpose them. From this point of view, the idea of the Brazilian system, illustrated to us by Eric Do Val Lacerda Sogocio, is certainly interesting, it must be deepened, it must be calibrated and thought out the in context of the individual state systems.

After all, it is crucial to involve the private system in this area. I must mention in this regard that stakeholders private took an active part in UN negotiations, were represented and spoke. We did a lot of negotiations and, in this sense, my memory goes back to the various informal meetings we had at the permanent representation of the United States at the United Nations, where we often discussed with the spirit that characterises the best Western

democracies of always having the bar of the guarantee of human rights and freedom of opinion in mind, which is fundamental to the success of this negotiation which, I repeat, is a compromise text.

Then there are other rules of the Convention that certainly cause concern. Professor Severino, in her speech as former Minister of Justice, stressed the danger that the rules of the Convention allowing the transfer of trials and the duplication of proceedings could generate, in the application phase, jurisprudential uncertainties But as a jurist, as a magistrate, I would like to say that we have to reckon with a concept of jurisdiction that the reality of the facts has totally unhinged. Those who thought of jurisdiction through the outdated idea of a link with the territory of a state, of a link with what happens in a state, in the face of cybercrime and the related new forms of crime must necessarily come to terms with a concept of jurisdiction - a sort of 'fifth dimension' - that is difficult to capture, borrowing an expression from an old prosecutor.

The aspect that seems most interesting to me is to understand how one can operate in this different environment, and this is precisely through the assistance that the server providers must provide, without entrenching themselves in the fact that the law allows data to be spread across several servers. So Eric's idea, peculiar to the Brazilian system, according to which is needed a legal representative in each country to take responsibility for what the provider does, is an idea that, in my opinion, deserves to be explored in the coming months. The doctrine will certainly make its contribution on this aspect.

I believe that the result achieved in terms of the obligations to criminalise even child pornography against minors is also extremely positive, a step that many have underestimated, but which I want to mention here, because there is a clause in Article 14 that penalises the production, offer, sale, distribution, and dissemination of child pornography material involving minors under the age of 18.

The concept of protection referred to, is all in that little aside inserted in the Conventionwithout right. It took a lot of effort to insert the phrase *without right.*

The Mauritanians and the Iranians, for example, demanded that a photo with sexual content of a minor should always be punished, always and in any case, because it was contrary to their religious , even when it was made freely by a minor who had full capacity to perform sexual acts and without any form of exploitation. There was a vote on this rule, it is one of the very few rules on which Iran asked for a vote, and when it lost the first vote it even proposed an amendment that said: "Well, at least give us the right to administratively punish, to administratively sanction this type of conduct, because in any case

a minor who, even using his freedom, has sexual relations with another partner and even takes a nice picture of himself, must still be punished." Here, a vote was also requested on this. This shows that the draft of the UN Convention, which I hope will be approved and perhaps even improved, has a mechanism of additional protocols on which there was an ideological and political battle, because people said: "But how, we approve a convention and we already foresee the possibility of amending it?"

Well, this was due to an, in my opinion intelligent policy ,of the president, Ambassador Faouzia Boumaiza-Mebarki, who, at a certain point, having the need to close the negotiations, gave this option. This option is certainly thought of by the groups of countries that were objectively defeated by the approval of this text, with all those firewalls, all those walls, all those barriers that we managed to insert, even bordering on pedantry, because in each chapter the rule concerning the protection of human rights was reintroduced. Even somewhat redundantly, Article 6, paragraph 2, was repeated in Articles 24 and 35. We have taken care in every area to insert this block, which will serve to avoid, I hope, Professor Milanovic's very justified concerns about - let us call them - .degraded democracies I like, perhaps using a neologism, to call them *democracies*, that is, a kind of vision of a kind of dictatorship that is, after all, founded on consensus, albeit a drugged consensus, a forced consensus.

In the end, however, I believe that a reasonable result was achieved, but above all, in the context of such a complex negotiation, the only technically possible result was achieved, respecting the red lines of Western democracies. This is a way of saying that my entire delegation and I were very proud to be able to offer our cooperation in confirming the limits of Western democracies in respecting human rights, in a Convention which, I must remind you, began with the intention of the Russian Federation and China to equip themselves with an instrument that could force Western democracies to cooperate in pursuing their dissidents even outside their country. And this, thank God, is a risk that has been avoided.

THE FUTURE IN UN CONVENTIONS. COOPERATION IN VIRTUAL SPACE - EFFECTIVENESS OF UN CONVENTIONS AND MODEL LAWS IN TRANSNATIONAL CYBERCRIMES

Glen Prichard
Chief of the Cybercrime Section, UNODC

It is my pleasure to be here today and to have the opportunity to provide an overview of the draft United Nations Convention against Cybercrime: particularly in relation to its intent to provide a framework on effective international cooperation in the virtual space.

This draft convention is the result of a Member States driven process, spanning over 5 years, involving 155 nations. It was approved on 8 August this year, by the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, which was tasked with elaborating the draft convention by the General Assembly. The text is still a draft and is expected to be considered by the General Assembly by the end of this year. Once adopted and entered in force, it will become the first legally binding instrument on cybercrime negotiated at the international level and the first United Nations criminal justice convention in over 20 years.

The draft convention is a crucial response by Member States to the challenges faced by law enforcement agencies in their fight against cybercrime. These technical and legal challenges are not new.

From a technical perspective, virtual space has become a major hub for criminal operations, with projected annual global costs reaching 10 trillion USD by 2025. Cyber-criminals exploit this virtual space, operating remotely and anonymously through tools like VPNs, encryption, and botnets. Artificial intelligence further exacerbates these crimes, by enabling ever more sophisticated scams and more

potent malware. The resulting evidence in electronic form, both for cybercrime and other serious crimes, may be scattered across jurisdictions and is inherently vulnerable to loss or manipulation.

On the legal level, law enforcement authorities fight a crime that knows no borders and can only act within their State's own territory. However, for their investigations and prosecutions, they depend on obtaining electronic evidence that is dispersed across jurisdictions and requires measures that may prejudice essential interests of states or bear the risk of abuse, potentially vi-

olating human rights. Ladies and gentlemen, putting this more plainly, the international community is charged with the responsibility of developing a solution to combat the proliferation of cybercrime in a paradigm where "*criminals operate at the speed of money and law enforcement operates at the speed of law*". An effective response to cybercrime therefore requires a framework for international cooperation, which balances enforcement necessities to establish common standards and new procedural tools, on the one hand, with safeguards that mitigate risks to national sovereignty and other essential interests, on the other.

The subject of my presentation will be how the draft UN Convention against Cybercrime attempts to accomplish this balancing act, by providing tools for effective enforcement through cross-border cooperation while providing safeguards that allow states to protect their national interests.

Convention - proposed slide: structure of the Convention

The draft convention follows the typical structure of an international criminal justice instrument:

- A chapter on criminalization, in which States Parties commit to criminalize certain conduct;
- A chapter on procedural measures, which updates the means and methods of criminal investigations at the domestic level, in order to investigate and prosecute these offences;
- A chapter on international cooperation, which "internationalizes" these procedural measures for evidence-exchange, and establishes mechanisms of international cooperation to further domestic criminal proceedings;
- In addition, the convention establishes provisions on preventive measures, technical assistance and capacity-building and a mechanism of review for the implementation of the convention.

General safeguards for sovereignty

The draft convention explicitly mandates the respect for sovereignty [article 4]. The principle of sovereignty applies equally in cyberspace, in both its internal and external aspects. Internal sovereignty refers to the sovereign authority of States over cyber infrastructure, individuals and cyber activities within their territory. External sovereignty relates to the freedom of States to engage in cyber activities in their international relations, and to enter into international agreements, including such on cybercrime.

In the context of this criminal justice convention, sovereignty is reaffirmed as States retain their role as primary interpreters. They retain discre-

tion in how to implement the convention within their national legal systems and according to their own legal principles. Moreover, States parties apply their own domestic laws in responding to mutual legal assistance requests. Finally, as reservations are not prohibited, they are permissible provided they are not incompatible with the object and purpose of the treaty. Sovereignty naturally does not mean freedom from law, but freedom *within* the law. The draft convention forms part of the entire corpus of international law and is governed and defined by the obligations States parties have consented to assume in their international relations. The draft convention also contains explicit references to other international frameworks. This includes the reference to the "purposes and principles of the Charter of the United Nations" [PP 1]. It also refers to "international human rights law" [articles 6, 24], affirming the application of international and regional human rights conventions as well as customary international human rights law. These references establish explicit minimum standard for the interpretation and implementation of the convention. Also, other treaties and obligations that are in force continue to apply, such as the Budapest Convention.

Jurisdiction

Closely related to sovereignty are the rules of jurisdiction, to which cybercrime presents a unique challenge, illustrating both the limits of territorial sovereignty and the potential for jurisdictional conflicts between states. As criminals operate across borders, multiple bases of jurisdiction – territorial, nationality-based, or effects-based – may lead to overlapping claims to legal authority in prosecuting these transnational offenses. The jurisdictional provision of the draft convention [article 22] establishes the legislative jurisdiction of States parties. It delineates the power and competence of States parties to subject persons (or property) to their laws and enforce them.

The mandatory bases of jurisdiction are based on territoriality, i.e. that some element of the offence has been committed in the territory of a State party [article 22.1(a)] [and its variants, e.g. flag state jurisdiction, article 22.1(b)]. Optional extraterritorial bases include the active and passive nationality principle [article 22.2(a-b)] as well as the protective principle, that is if an offence is committed against a State party [article 22.2(d)]. By allowing for these different jurisdictional bases, the convention strikes a balance between enabling effective prosecution of transnational cybercrime and preserving each State's sovereign right to exercise authority within its borders and over its nationals. States are also required to consult with other interested parties to minimize improper jurisdictional overlap when prosecuting transnational cybercrimes [article 22.5].

Criminalization

In accordance with these jurisdictional principles, the draft Convention calls on States parties to establish 11 offences in accordance with their domestic law [articles 7-17]. These offences reach from cyber-dependent crimes, such as illegal access to ICT25 systems and the illegal interception of electronic data to cyber-enabled crimes, such as offences relating to child sexual abuse and exploitation material and the non-consensual dissemination of intimate images. Committing to the criminalization of certain conduct naturally engages [internal] sovereignty, as it involves the power to define and enact criminal laws. However, the harmonization of criminal laws across jurisdictions is essential for facilitating international cooperation and meeting the dual criminality requirement, which ensures that a State is only obligated to assist in cases where the act in question is a crime in both the requesting and the assisting country. At the same time, states retain the right to apply their own legal principles when implementing these criminalization provisions. While States agree to criminalize these offenses, they retain discretion in how to incorporate them into their national legal systems.

Procedural measures

The investigation and enforcement of these offenses across borders encounter both jurisdictional and technical difficulties. Technical difficulties arise from the nature of electronic evidence, which is often volatile, dispersed across jurisdictions, and held by various service providers. This means that, in most cases, states depend on private sector entities for obtaining the evidence needed for their investigations and the cooperation with those States these service providers are established in.

Therefore, the draft convention also contains new procedural measures to adjust traditional means and methods of investigation to the ICT environment. These procedural measures require States parties to ensure that, at the domestic level, their authorities are able to expeditiously preserve [for up to 90 days] or obtain electronic data, through their law enforcement or with the assistance of service providers. These measures also foresee the real-time collection of traffic data and the interception of content data, which are critical in countering cybercrime. The real-time collection of traffic data enables law enforcement to trace communication routes from victims back to perpetrators, a capability essential in various scenarios. For instance, identifying the source of an intrusion in cases of illegal access, or tracking the distribu-

25 TIC equivale a "Tecnologie dell'Informazione e della Comunicazione, acronimo italiano dell'equivalente anglofono ICT

tion chain of child sexual abuse materials, would be nearly impossible without this tool. Equally important is the interception of content data, which allows law enforcement to assess the nature and legality of communications. Without content interception, it is often impossible to determine whether a communication is illegal. Such procedural measures have the potential to interfere with human rights, in particular the right to privacy and the freedom of expression. To balance these concerns, it incorporates safeguards allowing States to restrict such measures. These restrictions can be applied through reservations specifying certain categories or by limiting measures to serious criminal offenses as defined by each State's domestic law. Moreover, the draft convention mandates safeguards that are in accordance with the domestic law of states parties, as well as the principle of proportionality, which is informed by applicable human rights obligations.

[International cooperation]

Jurisdictional constraints in enforcing cybercrime arise as enforcement jurisdiction ends a State's own borders, and extraterritorial enforcement requires the consent from the relevant State for extraterritorial enforcement actions. Therefore, these procedural measures are "internationalized" through corresponding provisions in the chapter on international cooperation, allowing these investigative tools to be extended across borders through mutual legal assistance requests between States. This means, for instance, that one State can ask another to compel a local service provider to intercept content data for a criminal investigation. It is also foreseen, that one State can request another to quickly preserve electronic data related to a cybercrime investigation, before seeking formal access through mutual legal assistance procedures. In addition, the draft convention [article 35.1(c)] also foresees the exchange of electronic evidence for serious crime in general. In other words, any evidence in electronic form that could prove the commission of a serious crime could be shared between states, thereby substantially strengthening international cooperation in criminal matters. As in virtually every criminal case nowadays involves electronic evidence, this tool could revolutionize international cooperation in criminal justice matters. However, such a far-reaching framework on evidence-exchange has also raised concerns, which are counterbalanced by constraining this tool by human rights law: the draft convention [article 6, paragraph 2] explicitly exempts activities that constitute the exercise of human rights from its scope. Moreover, the provisions on mutual legal assistance [article 40, paragraph 21 and 22] contain broad grounds for refusing cooperation. Accordingly, cooperation may be refused if the request would prejudice the state's sovereignty, security, public order, or

other essential interests as well as if executing the request would be contrary to the legal system of the requested state. These grounds for refusal provide ample latitude for sovereignty considerations and may also encompass specific human rights concerns and political offense exceptions, thereby balancing international cooperation with the protection of national interests and fundamental rights.

Finally, a provision on the protection of personal data [article 36] allows refusal of cooperation if the requesting State lacks an equivalent data protection framework or cannot guarantee data use under conditions specified by the requested State. With respect to the stage of criminal proceedings and the exercise of adjudicative jurisdiction, the draft convention [article 37] also contains an extradition provision. Typically, for the exercise of adjudicative jurisdiction, the physical presence of the accused before domestic courts is required [, unless states resort to *in absentia* trials]. As a safeguard, extradition may be refused if there are substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on discriminatory grounds.

Preventive Measures and Technical Assistance

In order to provide a comprehensive framework against cybercrime, the draft convention also contains provisions on preventive measures [article 53] and technical assistance [article 54-56]. Most of them are optional or semi-mandatory, and/or to be implemented in accordance with and subject to domestic law.

The What difference does it bring?

Ultimately, the convention's proposed tools have the potential to revolutionize the global response to cybercrime, fostering unprecedented levels of international cooperation while respecting sovereign prerogatives. As the convention would be open to all States upon adoption, it could significantly enhance global efforts to counter cybercrime. More States parties would mean more international cooperation between law enforcement and less safe havens for criminals. It would also revolutionise the global fight against crime generally by strengthening international cooperation for the exchange of evidence in electronic form for serious crime involving such evidence.

The comprehensive scope of the draft convention and its far-reaching cooperative measures are carefully balanced by a range of robust safeguards. These safeguards are designed to mitigate potential risks to state sovereignty and national security, ensuring that international cooperation in combating cybercrime does not compromise the fundamental rights and interests of par-

ticipating States. International cooperation would thus not only lead to less crime internally, but also increase trust within the international community, diminishing the risks that few states resort to unilateral enforcement actions against cybercrime, which could in turn violate state sovereignty. While the draft convention may not be the utopia that will eliminate cybercrime, it will form an important part of a continuing efforts to combat crime, both online and offline, to ensure equal freedom for everyone and a more peaceful international digital environment.

DEBATE

Stefano Mogini:

I would also like to call for and open a debate, giving everyone the opportunity to speak. Naturally, the floor goes first to Attorney General Giovanni Salvi. Please.

Giovanni Salvi:

Ambassador McCarty's report touches on exactly the issues that were intended to be highlighted, including the differences in approach; it is so broad and in-depth that it should be well absorbed.

It would be interesting to urge Dr. Sogocio to reflect on the effectiveness of judicial cooperation under the forthcoming UN Convention compared to the Budapest Convention. Yesterday it was said that the draft of the new Convention, which is in the process of being approved, would represent a step backwards compared to the Budapest Convention, because it would not allow direct action by states in certain, albeit specific, areas, which is instead possible under the Budapest Convention. I would like to ask whether you share this view; in other words, is this the result of a need for mediation, or are the two approaches in fact substantially similar? And, in any case, do you think they are sufficient to address that specific issue that is different from cooperation in a general sense on the web. I am referring to those specific behaviours that require immediate intervention to reconstruct the trace of the origin of an attack, without having to wait for the consent of the attacking state.

Eric Do Val Lacerda Sogocio:

The question is: How does the new convention relate to the Budapest Convention? And how will it help countries to access information, request and receive data necessary for legal proceedings?

The crucial point is that we now have the possibility of involving all countries in a common system and therefore in a single regime for requesting and receiving information. It should also be emphasised that the countries that signed the Budapest Convention expressly stated from the outset that the new Convention should be seen as complementary to the Budapest Convention.

For countries already party to the Budapest Convention, it is now possible to have an additional instrument to use. For countries that are not party

to the Budapest Convention, on the other hand, the new convention offers an instrument that allows them to cooperate in a similar way to the Budapest Convention.

As Ambassador McCarty said, the UN Convention process could also stimulate accession to the Budapest Convention. We, as Brazil, understood from the beginning that not all countries would join the Budapest Convention and that a UN treaty would be necessary.

I believe that the added value of the new convention is precisely this: we now have common ground, a harmonisation of legislation and procedures. This offers the possibility of more effective and timely cooperation.

Finally, I would like to highlight the issue of capacity building, i.e. giving countries the opportunity to improve their systems.

Marko Milanovic:

It is fair to be proud that the negotiations, in which some of our interviewees participated, resulted in the adoption of a final text. However, one should not present the picture in such a rosy way. I think it is dangerous to present the Convention as a technical and apolitical method of cooperation between states on final issues when we all know how easy it is to circumvent criminal law for political reasons.

I, as a human rights lawyer, think that there is a great risk linked to the Convention. For example, looking at Italy, Italian magistrates will get used to working with the Serbian authorities with very little difficulty, while in Serbia, where democracy is deteriorating year by year and the government persecutes political opponents, responding immediately to requests for judicial assistance may mean becoming accomplices in human rights violations and unfair trials. This is a very high risk and should not be underestimated.

I agree that one must be vigilant. Eric is your point of view when you said that Brazil exercised its jurisdiction over Elon Musk's X but you can apply the law of companies operating in a territory because they offer services to users but in the example you gave there is a dark side: there was a judge who decided to suspend Twitter and who ruled that any Brazilian citizen who uses VPN to circumvent the blockade will be liable for a crime. China does it, India does it, it is a risk and a danger. So we should not approach this as a matter of pure technical cooperation; it is also a political issue and when training judges, prosecutors and police officers, they must know that there is always a political dimension.

Marco Roscini:

Question for Ambassador Giacomelli. Since you mentioned countermeasures, I was wondering whether Italy had an official position on so-called collective countermeasures, i.e. whether it believes that a State that is not a victim of cybercriminal operations can adopt countermeasures to help a State that is a victim of those malicious operations, or whether it believes that only the victim State can react. Italy is silent on this point in the *position paper*, so one wonders whether Italy has since developed an official position on this point.

Orestes Pollicino:

In this debate we see that the judicial dimension is only one part of a much bigger picture. I well understand Prof. Milanovic when he says that this approach is similar to that of Iran, but the Brazilian stance, at the level of human rights protection on the Internet, is pioneering. What I think is very important, we see it also in Europe, is to put together a judicial acceleration that can act as a boomerang with the framework regulatory that gives the principles of certainty also a good faith as far as the future is concerned for me it is important to combine the different ingredients especially for the Brazilian dimension.

Deborah McCarthy:

I wanted to respond to the concerns raised about the possibility that the process in the new Convention could be abused. Prof. Milanovic is absolutely right. In fact, we got a document that aims to protect the situation, because the level of trust was lower than the initial concerns. We tried to include as many safeguards as possible. For example, a proposal from Rica Costa ended to allow refusal of extradition for political offences, but we felt this could create problems and it was not approved. There are, in fact, several ways in which countries can refuse extradition, even under political pressure. This poses a challenge, especially considering that some countries may always refuse to hand over their nationals.

There is also another aspect that we have not been able to cover: the protection of cybersecurity researchers and other practitioners. As you know, there is no specific legislation on this, except in Belgium, and there are no such laws in the United States. Operations in this field take place in different ways and we could not introduce this protection through an international instrument such as the one we are creating.

However, we have included a chapter on prevention. Article 3 also provided for the possibility of covering those whom we do not trust, preventing

them from escaping justice simply by claiming to be *researchers*. This is a concern of the IT industry, as well as of journalists who might find themselves in risky situations during their travels. Unfortunately, there is still a regulatory vacuum in this area that needs to be filled.

We have built into the system some elements for monitoring the process, but proposals have been made, especially in the US, to create a public-private monitoring mechanism involving industry and human rights representatives. This could allow information to be gathered more quickly than we can, enabling us to take more timely action. Although the process is not perfect, we are considering the creation of a monitoring group, an idea that will be interesting to follow up on.

Stefano Mogini:

The issue raised by Professor Milanovic is certainly very important. I am reminded of how Italy, in its jurisdiction, uses the protection clauses against discrimination, which are also present in the UN Convention on Cybercrime, in a serious and accurate way. I believe that this can constitute, at least for our country, a solid defence against abuses that could emerge in any requests for judicial cooperation based on the new convention, providing an effective defence.

Eric Do Val Lacerda Sogocio

Professor Milanovic is absolutely right. When I wrote this text, I had exactly this in mind. Perhaps it is a little too optimistic and does not take into account problems that may arise, such as political difficulties. I remember hearing from a non-Western country about human rights protections: "We don't care, you can put in whatever you want, I know Western countries won't cooperate with us anyway." In essence, they said they were certain that, regardless of the text of the convention, those western countries would never cooperate, even if there was a very clear case and the requirements were met.

Regarding the convention, I believe that important steps forward have been taken. When you talk about the Brazilian Supreme Court and how the decisions were made, I would like to add that in Brazil we have the rule of law and during the negotiations I saw that many civil society institutions were trying to study the Convention as a useful instrument to create greater institutionalisation in the country and to promote the construction of the rule of law. the But Convention cannot do these things; it is an instrument, and I believe, in line with what Ambassador McCarthy said, that we need to be vigilant. The Convention has provided tools to monitor countries and make reviews. We hope to include civil society in this process. There are different methods of

monitoring under the Convention, but it is still worth having a Convention. When someone says that perhaps a world without the Convention would be better, I think they are wrong. With the Convention, we have ways to cooperate, which without it would not be as good.

VIRTUAL SPACE: CHALLENGES FOR MULTILATERAL JUDICIAL COOPERATION, THE BUDAPEST CONVENTION AND THE DRAFT UN CONVENTION ON CYBERCRIME

Antonio Balsamo

Former President of the Court of Palermo - Judge on the Roster of International Judges of the Kosovo Specialist Chambers

The new challenges of organised crime in virtual space

"A huge, boundless, unexplored world": this is the feeling Giovanni Falcone had about the Mafia when Rocco Chinnici entrusted him with the Spatola trial, the first trial in which a decisive breakthrough in the enhancement of international cooperation would be experienced.[26]

It is the same feeling one has today when confronted with the new face that organised crime has taken on in virtual space, in that cyberspace that has promoted inclusion worldwide, broken down barriers between countries, communities and citizens, made interaction and the global exchange of information and ideas possible, but, at the same time, created many vulnerabilities.[27]

This last critical issue is certainly of a general scope: as the then EU counter-terrorism coordinator Gilles De Kerchove pointed out back in 2019, "*the vulnerability of citizens, economies and governments increases proportionally to their connectivity and interdependence*"[28].

This trend is even more evident with respect to transnational cybercrime, which is now characterised by at least five innovative aspects that are further enhanced by artificial intelligence, namely

- wide-ranging offensiveness
- dematerialisation
- deterritorialisation

26 G. Falcone, interview, in Rapporto sulla mafia degli anni Ottanta, edited by L. Galluzzo - F. La Licata - S. Lodato, Flaccovio editore, Palermo, 1986: "the mafia, seen through the Spatola trial, appeared to me as an enormous, boundless, unexplored world (...) the papers of the Spatola trial contained a great reality to be deciphered. To get to the bottom of it, I used tools that already existed but that few had sufficiently utilised. An example: but was it enough to investigate in Palermo, in Sicily, in Italy? If the police here seize a load of drugs destined for the USA,' I asked myself, 'why not go to the USA to study the side effects of that successful operation?

27 Thus F. Spiezia, Cyber Threats and New Paradigms of International Judicial Cooperation: The Role of Eurojust, in Sistema Penale, 14 July 2023.

28 G. De Kerchove, intervention in the Justice and Home Affairs (JHA) Council meeting on 6 and 7 June 2019.

- speeding up
- detemporalisation.

A great magistrate such as Giovanni Salvi, who has succeeded in broadening the cultural horizons of the world of justice and innovating in depth the tools for combating transnational criminal phenomena, emphasised that *cybercrime* constitutes today's most serious challenge, due to its diffusion in every sector and its threat to the vital infrastructure of the community[29].

A recent, in-depth reconstruction by two of the leading experts on organised crime[30], reveals three evolutionary trends in the way the mafia operates that have occurred over the last eight years, which call for a corresponding adaptation of law enforcement strategies through the use of the most modern technologies.

The first factor of change began in 2016, when on the *social media* "Google Generation Criminal", made up of young people born at the turn of the century, landed. With this increasingly massive presence, social platforms become the theatres of a presidium strategy, similar to that used in the physical world: they become the engine of a continuous renewal of the mafia subculture, which redefines old paradigms, promotes a sort of post-truth, and builds consensus, a sense of identity and belonging, through a predominance of the aesthetics of wealth (which has a special attractive value in the territories of school desertification and prevailing unemployment) and an idealisation of the role of mafia exponents, perceived as providers of protection and problem-solvers for the communities in which they operate, in other words as "anti-heroes" leading the rebellion against a society that produces inequality and marginality.

The second shift, clearly manifested from the years 2018-2019 onwards, is the tendency of some of the most powerful mafia-type criminal organisations to channel their money flows into informal channels, through the cryptocurrency circuit, both for the conduct of illicit trafficking and for money laundering activities.

Finally, the third stage, which emerges in the years 2020-2021 with the first results of the investigations conducted on the platforms Encrochat and Sky ECC , concerns the use of "cryptophonins", supplied to a customer base of several tens of thousands of people by providers that have implemented extremely sophisticated communication encryption systems.

---

29 G. Salvi, Opening Speech at the Conference of the Attorneys General of the Member States of the Council of Europe, in Questione Giustizia, 23/5/2022.

30 N. Gratteri - A. Nicaso, Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta, Mondadori, 2023.

These are technical solutions aimed at neutralising all investigative tools, tried and tested up to then, for capturing conversations and messaging: both the "traditional" ones (such as telephone tapping) and the technologically advanced ones (implemented, for instance, by installing a "computer capturing device", i.e. a *Trojan* horse, on a *smartphone*).

Cryptophonets are devices in which the typical functions of ordinary *smartphones* are deactivated, such as Google services, the camera, the microphone, the Bluetooth system, the USB port, and the geolocation system. They are not hooked up to the normal telephone or telematic network because, in order to communicate, they use encrypted computer platforms whose operation depends on the use of *servers* privately managed located abroad. Hence the need for encryption keys, in the absence of which exchanged communication flows appear as sequences of numbers devoid of any intelligible meaning.[31]

These extremely expensive devices were used by tens of thousands of people, including more than 7,000 in Italy. Following investigations carried out by joint investigation teams set up by the French, Dutch and Belgian authorities under the coordination of Eurojust, their messaging devices have been used in a number of proceedings initiated in Italy, mainly concerning international drug trafficking run by members of the '*ndrangheta* and foreign clans (such as the Albanian ones) operating in our territory. Their evidentiary use is at the centre of a series of controversial issues that have been submitted to the judgement of several Supreme Courts of the Member States[32] , including our Court of Cassation[33] , and of the Court of Justice of the European Union[34]: a new and very delicate front within the already heated debate on the relations between the means of searching for evidence and the new technologies.[35]

It is in this context that "organised cybercrime is developing" , which could make use of the potential offered by artificial intelligence in the near future with extremely alarming consequences.[36]

If these are the most recent challenges posed by the globalisation of crime, on the triple level of collective culture, the economic dimension and

---

31 L. Ludovici, I criptofonini: sistemi informatici criptati e server occulti, in Penale Diritto e Procedura, Rivista trimestrale, 2023, n. 3, p. 417-418.

32 Cf. the overview traced by S. Ragazzi - F. Spiezia, Deciphering, acquiring and using encrypted communications in use by organised crime: a European look, pending the Italian countdown, in Sistema Penale, 26 February 2024.

33 See the judgments of 29 February 2024, No. 23755 and No. 23756.

34 See the Grand Chamber's judgment of 30 April 2024 in the M.N. case, on a reference for a preliminary ruling from the Landgericht Berlin.

35 L. Ludovici, op. cit., p. 417.

36 See A Balsamo - A. Mattarella, The Palermo Convention twenty years after its entry into force: new challenges and new perspectives, in Il diritto penale della globalizzazione, 2023, no. 2, p. 147 ff.

communication tools, there is no doubt about the need for a common commitment that must involve all institutions, with the same open-mindedness that marked the activity of a great magistrate capable of grasping the deep meaning, the socio-cultural roots and the interconnections of the criminal phenomena he investigated, such as Vittorio Occorsio.

From intergovernmental cooperation to new models of transnational circulation of electronic evidence

The use of electronic evidence in criminal proceedings covers a much wider area than the now traditional categories of cybercrimes in the narrow sense (which necessarily presuppose processes for automating data and information) and cybercrimes in the broad sense (which actually take place more and more frequently through the use of information technology, although without necessarily requiring it: already in 2019, the European Commission pointed out that "more than half of criminal investigations require access to cross-border electronic evidence", as "electronic evidence is needed for about 85 % of criminal investigations, and for two-thirds of these investigations there is a need to obtain such evidence from online service providers based in another jurisdiction".[37]

As one of the Italian magistrates with the most international experience has observed[38], the innovative features of electronic evidence - its peculiar location in several environments of the digital world, even subject to different jurisdictions, the private sources (*Internet Service Providers*), from which it frequently originates and where it can be found, the transnational nature of the crime in which it often becomes relevant, the need for high-tech investigative tools for its acquisition and for the intelligibility of the data it contains, its volatility and its limited duration in time, with the consequent need for its preservation - these are all factors that pour their load of novelty on our ordinary conceptual and normative paradigms, leading to the conclusion that we are in the presence of a second Copernican revolution in judicial cooperation, after the one that saw the transition from the intergovernmental dimension to direct relations between judicial authorities, with the forms of mutual recognition.

---

37 See Recommendation for Decision a Council authorising the opening of negotiations for an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final.

38 F. Spiezia, Cyberthreats and new paradigms of international judicial cooperation: the role of Eurojust, in Sistema Penale, 14 July 2023.

The most careful doctrine[39] has proposed a distinction between four forms of transnational circulation of electronic evidence:

a) the "evidence transfer" model, in which one State requests another State to transmit evidence that the foreign judicial authority has already come into its own possession for the purposes of domestic proceedings and is therefore "pre-constituted";
b) the "transnational evidence-gathering" model, in which one state commissions another state (by rogatory, European Investigation Order, or by requesting the setting up of a joint investigation team) to carry out a specific evidentiary activity in connection with ongoing criminal proceedings;
c) the model of "cross-border investigations", typical of the (EPPO *European Public Prosecutor's Office*), in which the collection of evidence beyond the borders of the state in whose territory been launched investigation has is entrusted to a different territorial branch of the same supranational prosecuting body;
d) the model envisaged by Regulation (EU) 2023/1543, concerning European production orders and European orders for the preservation of electronic evidence in criminal proceedings, which will apply from 18 August 2026 and configures "electronic evidence" circulation modules that disregard the traditional horizontal cooperation mechanisms and, therefore, a dialogue between judicial authorities: in fact, in order to acquire data stored electronically abroad by a service provider operating in the European Union, the competent authorities will no longer have to request the intervention of the judicial authorities of the executing State, but will be able - on the basis of the principle of mutual recognition under certain conditions and if allowed for similar domestic cases - apply directly to the foreign service provider, to order it to produce (or retain) data relating to subscribers, traffic or content (including, the latter, "any data in digital format, such as text, voice, video, images or sound"), excluding interceptions.

Even following this latest regulatory intervention aimed at ensuring an efficient and comprehensive system of cross-border acquisition of electronic evidence, with a view to facilitating its circulation in the European judicial area, there is still a lack of harmonisation of national legislation on the rules concerning the admissibility and usability of evidence.

---

39 G. Di Paolo, The Cross-Border Circulation of Electronic Evidence, in Criminal Law and Procedure, 2024.

There continue to be, therefore, profound differences between the procedural systems of the EU Member States, which risk undermining the effectiveness of the new forms of judicial cooperation as well as hindering the protection of the fundamental rights of persons.[40]

The very recent definition of the text of the new UN Convention against Cybercrime

Awareness of the difficulties that the incessant evolution of cybercrime creates for the effective exercise of each country's national jurisdiction - a power traditionally applied in relation to criminal phenomena well defined in time and space - is leading the international community to design new forms of judicial cooperation, which may find an important legal basis in the near future in the United Nations Convention against Cybercrime, the text of which was approved on 8 August 2024 by the Intergovernmental Committee *Ad Hoc* in charge of the relevant negotiations and will be submitted to the UN General Assembly for final adoption next November.

The approval of what is destined to become the first UN convention on cybercrime took place without opposition from any state, but was accompanied by strong criticism from an unprecedented alliance of human rights defenders and large technology companies.

However, it should be noted that even in the context of an international organisation strongly committed to the protection of fundamental rights, such as the Council of Europe, the new UN Convention was seen as an important political achievement.[41] The very fact that the approval of its text was achieved by the method *consensus* (i.e. with substantial unanimity) is particularly significant if one considers that the start of the path that gave birth to the Convention had been marked by a conspicuous divergence of direction between Russia, which had formulated the relevant proposal accepted by a majority by the UN General Assembly in December 2019, and the Western states. Specifically, Resolution 74/247 had been passed with 79 votes in favour (including those of Russia, China, and most South-East Asian countries), 60 votes against (including those of the United States, the United Kingdom, Japan, Australia, and several European countries), and 33 abstentions.

In the course of the subsequent work, there had been no lack of reservations on the part of the European Union, the United Kingdom and the United States, which had pointed out the need to avoid any prejudice to the application of existing international instruments, of global or "regional" scope, which

40 G. Di Paolo, op. cit.

41 See Conventions on cybercrime: The Budapest Convention and the draft UN treaty, in www.coe.int

enable the effective combating of cybercrime, such as the Palermo and Budapest Conventions, and had stressed the need to include appropriate guarantees for fundamental rights, including freedom of expression. In the final stages of the negotiations, in turn, Russia had voiced some criticism of the text being drafted, considering it "over-saturated with human rights guarantees". Iran had tried, unsuccessfully, to have articles removed such as the one allowing states to deny requested mutual legal assistance if they consider the ongoing investigation to be discriminatory in nature.

The conclusion of the negotiation process, of which Russia claimed to have been an "inspiration and leader", was also welcomed by the United States of America, which emphasised that the agreement reached "broadens the global fight against cybercrime, which is one of the most pervasive challenges of our time, affecting communities around the world", and pointed out that "the Convention provides countries with additional tools to work together, including through law enforcement cooperation, to address cybercrime, including the protection of children". At the same time, the United States reaffirmed that it "will continue to strongly condemn and work to combat the persistent human rights abuses we see around the world by governments that misuse and abuse cybercrime laws and other cybercrime-related legislation and tools to target human rights defenders, journalists, dissidents, and others". [42]

As mentioned above, however, criticism has to be registered both from a number of NGOs engaged in the defence of human rights and from the Big Tech sector, which have warned against a tool that could lead to "global surveillance".

On closer inspection, the fears linked to the new Convention can only be effectively addressed by decisively enhancing the role of jurisdiction, which appears to be irreplaceable in ensuring a fair balance between all the fundamental rights involved.

The international legal framework in the making

After the adoption of the new Convention by the UN General Assembly, the international legal framework on transnational cybercrime will comprise three key instruments:

a) the United Nations Convention against Transnational Organised Crime, adopted in Palermo in 2000 and entered into force in 2003;
b) the Council of Europe Convention on Cybercrime, adopted in Budapest in 2001 and entered into force in 2004;

42 See press release of 9 August 2024 from the US State Department spokesman.

c) the UN Convention against Cybercrime, which is expected to be adopted by the General Assembly in November 2024 and enter into force three months after ratification by 40 states.

The Palermo Convention has a truly universal character, because it has 192 Parties (compared to 193 United Nations Member States). It is, however, a general instrument, which covers all forms of transnational organised crime (including any type of collective commission of serious offences - i.e. punishable by a maximum sentence of no less than four years - with perpetrators or effects in a number of countries) and is not specifically targeted at cybercrime.

The Budapest Convention, on the other hand, is specifically dedicated to cybercrime (also of an individual nature, of reduced seriousness and of a national dimension only), but it is not universal: it falls within what, in the legal language of the United Nations, are defined as "regional instruments"; it arose within the Council of Europe and currently has 76 parties to it, including several non-European countries (such as Argentina, Australia, Brazil, Canada, Japan, Morocco, Nigeria, the United States), but not, for example, Russia and China.

The new United Nations Convention against Cybercrime also specifically targets this criminal phenomenon, but is intended to be universal in scope, thus filling the gaps in the protection of legal assets inevitably linked to the limited *membership* (and consequently the territorial scope of reference) of the Budapest Convention.

Profiles of continuity between the Budapest Convention and the new UN Convention

An initial comparison between the Budapest Convention of the Council of Europe and the new UN Convention on Cybercrime highlights a number of aspects of continuity in the content of their provisions.

A) Firstly, both conventions provide for a largely overlapping set of "typical" cybercrimes: in particular, both criminalise the conducts of illegal access to a computer system, illegal interception, interference with electronic data, interference with a computer system, misuse of equipment, computer forgery, computer fraud, child pornography. To this are added, for the Budapest Convention, offences against intellectual property, and, for the new UN Convention on cybercrime, the crimes of cyber theft, *grooming, revenge porn*, and money laundering.

B) Secondly, both conventions require states to adopt such measures (legislative and otherwise) as may be necessary to establish a set of powers and procedures, to be compulsorily applied with regard not only to "typical"

computer offences, but also to all other offences committed through a computer system and to the collection of all electronic evidence of the various offences.

These procedural measures include:

a) the rapid storage of stored electronic data;
b) the rapid storage and partial disclosure of traffic data;
c) the production order;
d) the search and seizure of stored computer data;
e) the real-time collection of traffic data;
f) the interception of content data (with reference to a number of serious offences, to be defined in the laws of individual countries).

In the new UN Convention, to the aforementioned measures (which are constructed in a similar way to the corresponding measures governed by the Budapest Convention, also with regard to the confidentiality of transactions) are added, for "typical" cybercrimes, further provisions concerning the freezing, seizure and confiscation of the proceeds of crime, witness protection, and assistance and protection for victims.

C) Thirdly, the general principles governing mutual legal assistance are similar, which, however, in the new UN Convention - as compared to the Budapest Convention - is more limited in scope as regards the collection of electronic evidence (which is only referred to serious offences, i.e. punishable by a maximum sentence of no less than four years), and is characterised by a lower degree of bindingness (resulting in a more general commitment) in the areas of real-time collection of traffic data and interception of content data.

D) Fourthly, both conventions provide for the establishment of a 24/7 Network of always available points of contact to ensure immediate assistance in the field of international cooperation, with an objective area of operation that is more extensive in the Budapest Convention but with a richer "arsenal of tools" in the new UN Convention (which also refers to the provision of electronic data to prevent an emergency).

The human rights provisions of the new UN Convention

In the context of the new UN Convention on Cybercrime, the issue of the protection of fundamental rights remains crucial, which has been the subject of opposing assessments (the relevant regulation is allegedly deficient according to human rights NGOs, and oversized according to some states, such as Russia and Iran).

On closer inspection, there is an almost complete overlap between the provisions dictated by Article 15 of the Budapest Convention and those contained in Article 24 of the new UN Convention on Cybercrime, which regu-

lates the "conditions and guarantees" to which the powers and procedures applicable with regard to "typical" cybercrimes, all other offences committed through a computer system, and the collection of electronic evidence of the various offences must be subjected - not only in the context of investigations conducted at national level but also in the context of the provision of international mutual legal assistance requested by other states.

Precisely, with wording similar to paragraph 1 of Art. 15 of the Budapest Convention[43] , paragraph 1 of Art. 24 of the new UN Convention on Cybercrime requires each state to ensure that the establishment, implementation and enforcement of these powers and procedures are subject to the conditions and guarantees provided for in domestic law, which must provide for the protection of human rights, in accordance with obligations under international human rights law, and which must incorporate the principle of proportionality.

Obviously, in view of the different legal context of reference, Article 24 of the new UN Convention lacks an express reference to the ECHR, which is present in the Budapest Convention. The ECHR, however, represents one of the main sources of international human rights law and is productive of precise obligations, for the States that adhere to it, also with regard to the matter under examination. There is no doubt, therefore, that for such states, any regulations issued in implementation of the new UN Convention to further regulate the aforementioned means of obtaining evidence must comply with the ECHR.

This conclusion is reinforced by consideration of the text of Article 6 of the new UN Convention, which commits states to ensure that the implementation of their treaty obligations is consistent with their further obligations under international human rights law.

Also analogous to the provision of paragraph 2 of Article 15 of the Budapest Convention[44] , paragraph 2 of Article 24 of the new UN Convention states that, in accordance with and under the domestic law of each State, the conditions and safeguards, where appropriate having regard to the nature of

---

43 Specifically, paragraph 1 of Article 15 of the Budapest Convention is worded as follows: "1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this section shall be subject to the conditions and safeguards provided for in its domestic law, which shall ensure adequate protection of human rights and freedoms, in particular the rights deriving from obligations under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental , the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and shall take into account the principle of Freedoms proportionality."

44 The text of paragraph 2 of Art. 15 of the Budapest Convention reads as follows: "Where appropriate, having regard to the nature of the power or procedure, these conditions and safeguards shall include, inter alia, judicial or other independent supervision, the reasons justifying their application, and limitation of the scope and duration of the power or procedure.

the procedure or power in question, shall also include judicial or other independent review, the right to an effective remedy, the grounds for applying it, and the limitation of the scope and duration of such power or procedure. Indeed, the new UN Convention adds a reference to the right to an effective remedy, which was not included in Article 15 of the Budapest Convention.

Paragraph 5 of the same Article 24 specifies that the reference to judicial or other independent control refers to what is established at national level. This is, however, a superfluous clarification, as there are currently no supranational systems of preventive control over the means of obtaining evidence established in the context of criminal proceedings within individual States.

Finally, as far as the protection of third parties is concerned, the mild preceptive content of paragraph 3 of Article 24 of the new UN Convention ("In so far as it is compatible with the public interest, in particular with the proper administration of justice, each State Party shall consider the impact of the powers and procedures of this chapter on the rights, responsibilities and legitimate interests of third parties") fully corresponds to the content of Article 15 of the Budapest Convention.[45]

A concluding assessment therefore leads to the recognition that the provisions of Article 24 of the new UN Convention on Cybercrime do not in themselves entail a retreat in the protection of human rights compared to the standards guaranteed by Article 15 of the Budapest Convention.

What changes, rather, is the circle of states affected by the two international instruments: the greater breadth of the potential *membership* of the new UN Convention is clearly matched by a lesser homogeneity of the respective constitutional structures and guiding principles of their legal systems. It follows that identical provisions may be applied in profoundly different ways in the various legal systems.

This is a problem that should not be underestimated, but which, as things stand, can only find a gradual solution through two routes:

a) on the one hand, the development of a common human rights culture among the judiciaries of the various states; an objective that can be pursued by enhancing the tools of the "dialogue between courts" and *cross-fertilisation* between legal systems; on this front, the technical assistance activity that finds a significant space in the new UN Convention can play an important role;

---

45 Article 15(3) of the Budapest Convention provides as follows "3. To the extent consistent with the public interest, and in particular with the proper administration of justice, each Party shall consider the impact of the powers and procedures of this Section on the rights, obligations and legitimate interests of third parties."

b) on the other hand, the implementation of review systems that lead to the dissemination of best practices found in some countries, recommending appropriate regulatory and organisational reforms in the most problematic contexts; a task that falls within the remit of the Conference of the Parties to the new Convention.

On both these possible developments, an important role can be played by Italian "legal diplomacy", which in the recent period has been strongly engaged in technical assistance in favour of other countries and in the implementation of the revision mechanisms of the Palermo and Merida Conventions, enhancing the most modern positions of our judicial system.

The innovations introduced by Second Additional Protocol to the Budapest Convention and absent from the new UN Convention

Absent from the text of the new UN Convention are some important innovations introduced by the Second Additional Protocol to the Budapest Convention, which was adopted in November 2021 by the Committee of Ministers of the Council of Europe and will enter into force three months after ratification by at least five states.

The Second Protocol contains, in particular, a detailed regulation on the protection of personal data and the provision of procedures aimed at strengthening direct cooperation between state authorities and private entities, enabling the investigative bodies of a state party to obtain information, concerning domain name registrations and subscribers, directly from *Internet Service Providers* with their main or secondary offices in the territory of another country .[46]

The latter type of power, which closely resembles the fourth of the models of transnational circulation of electronic evidence described above, is not reflected in the new UN Convention.

The added value of the new UN Convention from the fourfold perspective of joint investigative bodies, law enforcement measures targeting the economic dimension of cybercrime, prescription of offences and extra-criminal instruments

Compared to the set of provisions contained in the Budapest Convention and its Second Additional Protocol, the new UN Convention on Cybercrime presents an important added value, inherent in the discipline dictated

46 The Second Protocol introduces also procedures to strengthen international cooperation between the authorities of different states for the disclosure of stored computer data, procedures on emergency mutual legal assistance, provisions on video-conferencing, joint investigation teams and joint investigations.

by Article 48, which requires States Parties to consider the opportunity to conclude bilateral or multilateral agreements or arrangements for the creation of joint investigative bodies, by the competent authorities, in relation to "typical" cybercrimes that are the subject of investigations, prosecutions or judicial proceedings in one or more States.

This is a provision with a content corresponding to Article 19 of the Palermo Convention, on which an elaboration of particular innovative relevance within the United Nations has been built.

In fact, the notion of "joint investigative bodies" can encompass a plurality of typologies, some of which have already been widely experimented with important results - as in the case of joint investigation teams - while others have yet to be widely explored and may give rise to systemic developments of extraordinary interest. From the coordination of investigations, one could move on to the creation of an official legal entity with its own investigative functions, complementary to the tasks of the investigative bodies of the individual states concerned.

This is therefore a methodology for organising investigations that closely resembles the third of the models of transnational circulation of electronic evidence described above and is not fully reflected even in the Second Additional Protocol to the Budapest Convention, which merely lays down provisions on joint investigation teams and joint investigations, without mentioning "joint investigative bodies".

In this regard, it should be noted that in recent years, within the Working Groups of the Conference of the Parties to the Palermo Convention, it has been emphasised that a distinction can be drawn between simple "*joint investigative teams*", formed to investigate specific cases within a limited period of time, and "*joint investigative bodies*", marked by a permanent structure and competent to investigate specific types of offences. [47]

The creation of joint investigation teams may be the most appropriate strategy to deal with the most problematic aspects of cross-border computer crime, as it can significantly speed up the judicial response, is free from territorial constraints and is capable of producing evidence that can be used in a variety of legal systems, based on the application of a widely shared set of guarantees.

Among the most significant features of the new UN Convention is the strong focus on the issue of the economic dimension of cybercrime, which

---

47 On this point, see the Background paper prepared by the Secretariat for the Working Group on International Cooperation meeting in Vienna on 7-8 July 2020 on: The use and role of joint investigative bodies in combating transnational organised crime.

has led to the inclusion of a number of provisions likely to give a considerable boost to the relevant judicial initiatives, such as those on international cooperation aimed at confiscation and the related recovery of assets (Art. 49 and 50), on special cooperation (Art. 51), and on the restitution and destination of confiscated assets (Art. 52).

Another significant provision introduced by the new UN Convention on Cybercrime concerns the issue of statute of limitations. Precisely, Article 20 obliges states, on the basis of consideration of the seriousness of the offence, to establish in their domestic law a long statute of limitations for the commencement of proceedings for any "typical" cybercrime, and to provide for the extension or suspension of the statute of limitations if the alleged offender has evaded the administration of justice.

This is a clear impetus for the introduction of suitable regulatory measures to avoid the statute of limitations for the offences in question, which, as is well known, are often dealt with within the timeframe of a trial that is liable to accrue this cause of extinction.

This provision is even more important, in our country, since the most recent case law of legitimacy is moving in the direction of considering as interposed parameters of constitutionality, in relation to Article 117 of the Constitution, also the international Conventions other than the ECHR and affecting criminal matters, such as the Palermo Convention and the Merida Convention.[48] This is an interpretative direction that can certainly be extended to the new UN Convention on Cybercrime.

Finally, it should be noted that the new UN Convention on Cybercrime adopts a broad strategy to combat this criminal phenomenon, not limited to criminal law instruments but extended to preventive measures (Art. 53), technical assistance with capacity building (Art. 54), and economic development (Art. 56).

---

48 In this sense, the principles affirmed by Cass. Sez. 5, no. 18837 of 01/02/2024, Rv. 286518, which pointed out that "the United Nations Conventions oblige the States Parties (including Italy) to take, to the greatest extent possible within their domestic legal system, the necessary measures to enable the confiscation of the proceeds of offences arising from the offences provided for therein, which include corruption (Article 12 of the Palermo Convention and Article 31 of the Merida Convention). It follows that the application of preventive confiscation to all rights of a patrimonial nature arising from contracts derived or obtained, directly or indirectly, through the commission of corruption offences, constitutes the result of an obligation to interpret domestic legislation in a manner consistent with the rules on confiscation and its object contained in the aforesaid international Conventions, which are certainly suitable, by virtue of their specific preceptive character, to take on the value of interposed parameters in relation to Article 117 of the Constitution". It was thus accepted "a conventionally compliant interpretation of the concept of proceeds of crime, made mandatory by the provisions of art. 117 of the Constitution".

What prospects for the future of cybercrime fighting

The now imminent approval of the new UN Convention in no way implies a "delegitimisation" of the instruments that have existed so far.

On the contrary, the international legal framework under construction can be hinged on a joint utilisation of the three international conventions, on which a gradual work of normative, interpretative and applicative osmosis can also be set up, with enhancement:

- of the most modern instruments and the rules on the protection of personal data contained in the Second Additional Protocol to the Budapest Convention;
- the perspective of joint investigative bodies outlined by the Palermo Convention and the new UN Convention;
- the role of the judiciary as guarantor of multilevel protection of the fundamental rights of all those involved is of essential importance also for the development of that mutual trust between the different legal systems that is indispensable for the strengthening of international judicial cooperation.

Also within the Council of Europe, the possibility of promoting a significant synergy between the new UN Convention and the Budapest Convention is strongly envisaged, in particular through activities *capacity-building* that would simultaneously involve the *Cybercrime Programme Office of the Council of Europe* (C-PROC) and the *United Nations Office on Drugs and Crime* (UNODC) and that could also take the form of support for the preparation of national legislation in various countries, with a particular focus on the issue of guarantees.[49]

In the present historical phase, it is becoming increasingly clear how important it is to steer the EU's forthcoming legislative output towards two now inescapable goals.

First, a broad harmonisation of the regulation of wiretapping and all modern means of interception of communications, not covered by Regulation (EU) 2023/1543, must be achieved.

In fact, precisely the most modern means of searching for evidence, which are essential for mafia investigations, have so far remained outside the process of regulatory harmonisation, which is instead of fundamental importance in order to adopt in all states (including Italy) those measures, both legislative and organisational, that are required by the enormous changes that are constantly affecting the world of communications and that organised crime is constantly exploiting.

---

49 See Conventions on cybercrime: The Budapest Convention and the draft UN treaty, in www.coe.int

Secondly, it is indispensable to prepare a detailed common framework on the liability of internet intermediaries, with specific measures covering all the most significant areas likely to be used by criminal organisations (various forms of messaging, social networks, artificial intelligence, cryptocurrencies, etc.), so as to eliminate the persistent uncertainties on the scope of the relevant obligations and non-punishability clauses, and to boost a modern and coordinated law enforcement strategy in this field.

Europe, if it succeeds in giving impetus to a common regulation in this sensitive but crucial area, can take a leading position in the implementation of the new UN Convention on Cybercrime.

DEBATE

Carmela Decaro

I am part of the Vittorio Occorsio Foundation in this last phase of its life, therefore as a true elder. However, I cannot fail to thank the Ministry of Foreign Affairs and the government for the extraordinary collaboration that has made these two days possible, and I cannot refrain from a reflection, to which the rapporteur Balsamo urged me most recently, on legal diplomacy.

In developing this very short speech, I refer, among the various opportunities of my professional life, to the period when, between 1997 and 1999, I was head of the International and European Union Relations Service of the Chamber of Deputies, and where I noted the extraordinary interest of the then President of the Chamber, Luciano Violante, in the construction of a "parliamentary diplomacy".

As a professor of Constitutional Law, I participated in the extraordinary season of dialogue between the constitutional courts that opened between the end of last century and this century and that led to extraordinary innovations, such as that of introducing into the South African Constitution the reference in the legal sources to the judgments of the constitutional courts of other countries.

Today I hear about the possibility of legal diplomacy and dialogue between jurisdictions, which is precisely the lesson of the United Nations. It is a lesson that needs to be translated more and more into practice.

My wish is that we find, as the Chambers and Parliamentary Assemblies of the world do and as the Constitutional Court does, more and more opportunities to institutionalise appointments, which are not touristic, but are about deepening content and human relations between jurisdictions as well.

The European Union, with the European Public Prosecutor's Office, is in the vanguard, but within these activities of monitoring, protocols and forms of review, the power of legal diplomacy - as Antonio Balsamo calls it and which I would call jurisdictional - is a channel to which I invite.

One last reminder. I read just a few days ago 's book Mink latest book, which is called *The Flattened World*. Well, one of the solutions that he proposes is the jurisdictionalisation, the focus on the individual case, which can lead to a channel for a democracy of the future that counteracts the flattening.

Stefano Mogini

Thank you, Professor. It seems to me that this is truly an open bridge to new reflections.

Enzo Bianco

Prof. Decaro has anticipated my thought: to applaud the institution that is crowning and sealing these intense and almost concluded two days on legal diplomacy, on the diplomacy of jurisdictionalisation, which I would call the diplomacy of the legal community.

The reaffirmation and warning, which I heard clearly yesterday and today, on the need to prevent - and, if appropriate, obviously repress - certain criminal offences, but always keeping in mind respect for the guarantees and, above all, respect for the human rights that unite us, is beautiful.

Professor Milanovic said it clearly, but reaffirmed it, perpetuating an *thread* ideal President Balsamo, this morning. As a lawyer - and lawyers do what they are supposed to do, defend the victims, but also the accused and sometimes the condemned - I reiterate that lawyers must certainly respect sentences, but at the same time always check that human rights are respected.

But there must be, as the professor said, a recognition of all the stakeholders involved, including the legal profession, which must stand by the institution in a fair manner.

I am in favour of overcoming sterile overlaps and contrasts between actors in the system, and I very much appreciate President Balsamo's very clear words in reaffirming the rights and guarantees that must also see lawyers, as defenders of the last and defenders of rights, as protagonists of the jurisdiction, together with the other actors in the process and, even before that, in the proceedings.

Andrea Venegoni

I am Andrea Venegoni, European Public Prosecutor for Italy within EPPO. I will make a very short intervention, since the European Public Prosecutor's Office (EPPO) has been evoked several times.

I want to share many of the points that have been made, also by Antonio Balsamo. EPPO is a very interesting "project", if we want to call it that, and I say this for those who come from a "non-EU" context, because it creates within the European Union a single European office and jurisdiction: a European investigation office. So the magistrates of EPPO are no longer magistrates of individual national jurisdictions, but they are magistrates working as European magistrates.

In the EPPO investigations, many of the problems that Antonio Balsamo mentioned arise and which, of course, in the supra-European dimensions arise in the same way and perhaps even more critically, such as the acquisition of evidence, the transfer of evidence and the admissibility of evidence in trials that are conducted in individual states.

However, at the same time, since EPPO deals with many transnational crimes, EPPO's competence, while not focused on cybercrime, is directed at crimes that can also be committed through cybercrime, such as money laundering.

The experience of EPPO may well pave the way or be kept in mind. Of course, it is not easily replicable outside the European Union, because EPPO could be established on the basis of principles common to and characterising the member states.

Obviously, as also emerged from today's speeches, the larger the size of the participating states in instruments or conventions, the more difficult it is to find a common basis.

But, at the same time, since EPPO moves within a legal and regulatory framework of the European Union and also outside Europe that is constantly evolving - and I am thinking, for example, of the possible extensions of EPPO's competence also to transnational crimes that go beyond its current competence - we feel part of this process.

I believe that the basis for the development of these instruments is always an important political will; a political will that the EU states achieved when it came to setting up EPPOs, and which is equally necessary when it comes to laying the foundations for transnational law enforcement instruments of an even higher dimension. And indeed, the broader the range of participants, the more difficult it is to arrive at a clear and specific political will.

But if, in some way, the experience of EPPO could be useful for the development of further tools or additional means to fight transnational organised crime, EPPO is certainly available and we would like to see it taken into account

ROUND TABLE

THE EFFECTIVENESS OF MULTILATERAL POLICE AND JUDICIAL COOPERATION IN CYBERSPACE - EXPERIENCES IN THE FIELD

COORDINATION

Eugenio Albamonte
Deputy Public Prosecutor - Rome

Before entering into the subject, I too would like to thank the Occorsio Foundation and in particular Eugenio and Vittorio Occorsio and Giovanni Salvi, who chairs the Foundation's scientific committee. I thank the Foundation first of all because it exists and, secondly, because, alongside its activity of civil commitment in the proactive memory of a dramatic period in the history of the country, which is that of terrorist violence and the use of brute force to assert one's own political vision, it is committed in many fields. This is a field that is particularly dear to me; I also thank you for having wanted to involve me with a small contribution on this day of such an important and strategic conference.

The effectiveness of multilateral police and judicial cooperation in space and experiences in this field are the focus of our meeting. Our round table can be above all a comparison of experiences. We will divide our time into two short communications for my speakers: a slightly longer one, of about ten minutes, and an inevitably shorter one, in which we would like, in a first round, to take stock, from different points of view, of the state of the art, i.e. how judicial cooperation has evolved, especially in this field. I would like to point out that, in just a few years, great strides have been made. However, there are also critical points that we are experiencing today. In a second round, we will address some ideas on possible ways to implement and strengthen judicial cooperation.

I have been working for about 15 years, at the Rome Public Prosecutor's Office, on cybercrime on investigations in cyberspace. A type of investigation that is and inevitably, therefore, intimately and inextricably linked to judicial cooperation, be it the simplest forms of cooperation or the most complex ones. It is a question, for example, of acquiring traffic data from an external or, on the other hand, in the most extreme, most serious, most compli-

cated cases, of identifying the operations of complex IT structures operating in different countries, which have criminal functions. Functions *internet service provider* that we often define as criminal only because, as has been said in several passages in these days, we are not sure of the attribution, or rather, we cannot with certainty often attribute to these actions the guise of criminality, but the nature of real hostile acts coming from foreign state structures, with respect to circumstances in which we often have elements of concrete and serious suspicion. But, precisely, the issue of attribution keeps this conduct in the context of criminal phenomena. The need for cooperation clearly emerges from the structure of cyberattacks. These, in fact, do not directly correlate the attacked critical infrastructure with the attacking one, but often use a series of infrastructures "proxy", i.e. linking and obfuscating, connected in various parts of the world.

In these 15 years, we have moved from an initially very cumbersome, bureaucratic, passive cooperation, with almost biblical waiting times, to an increasingly operational and performing cooperation, until today, with the tools available, we have reached a level of excellence. This has happened thanks to the evolution of cooperation instruments and thus to the introduction of joint investigation teams, European investigation orders, and the strengthening of the competences of Eurojust and Europol, represented at this round table by my colleague respectively Hannes Glantshnig (Eurojust) and Edvardas Sileris (Europol)

Another determining factor was the widespread and growing awareness within the various systems and states of the importance and seriousness of the cyber threat.

However, we cannot hide behind a finger: what really strengthens cooperation is the so-called "common enemy". In this historical phase, all European countries and many non-European countries, but nonetheless belonging to the cultural area of the Western democracies, are subjected to cyberattacks that mostly have the same motive, the same matrix and the same origin. It is evident that these dynamics strengthen the operability of cooperation.

Each of us, attacked countries, knows that a piece of evidence found through the analysis of an attacked server, or a computer trace, alone leads to nothing. However, put together with another piece of evidence, perhaps found in a Dutch, Canadian or US computer crime scene, it can help give a broader picture and enable a better ability to detect the attacker.

Today, therefore, we are witnessing cooperation that is almost like that between judicial offices of the same country, with very close meetings, whose function is not only to formally exchange information, but also to share strategies and plan investigative actions. We have judicial police teams operating

directly alongside local state police in theatres other than their own national ones. Thus, judicial police who move to access investigative activity together with the national police on foreign territory.

This obviously also determines a more general benefit: firstly, for the acquisition of evidence in ways that are more consistent with the legal systems of the various states; secondly, for the sharing of investigative practices in the field; thirdly, for the sharing of technicalities, structures and means, the latter being elements are thatas important context as the techniques. Thus, the dissemination of programmes that each judicial police brings with it and that are jointly used on a crime scene also leads to greater circularity of the underlying technicalities.in the

And yet, despite the progress made by cooperation in recent years, we are still unable to achieve optimal results. This is the theme that I would like to hand over to my interlocutors, whom I would like to ask first of all to take stock, together and each from different points of view, of the state of the art and the critical issues that, despite the positive aspects deriving from enhanced cooperation instruments, still .prevent us from achieving adequate results

Ivano Gabrielli

Director of the Postal and Telecommunications Police

Just a couple of thanks for the extraordinary opportunity to experience these two exceptional days of debate, as much for the level of the interlocutions as for the insights I will take away with me, dropping them into the operational activity that sees me heading the structure of the Postal Communications Police.

Former Minister Interior Enzo Bianco first mentioned the political vision that led Italy back in 1999-2000 to consider it necessary for there to be a specialised Cybercrime Corps within the State Police. In this regard, I salute Prefect Pansa*, who was the first interpreter of that design, a design that led us to be among the oldest corps* police dealing with cybercrime.

I remain within the confines of the topic entrusted to me, that of international police cooperation. It must be judicial cooperation, the flip side of the coin of what has been so painstakingly built around the UN Convention on Cybercrime. I have followed the work from the very beginning, I know the difficulties faced and also the initial diffidence of the various representations towards a proposed convention that came from a world so different from that of the so-called "LDCs". I understand the extraordinary importance of the result of having built a common ground with regard to the detection of cybercrimes.[50]

The reference made earlier to shifting the discussion from cybersecurity tout court to cybercrime, common ground where dialogue and cooperation find fertile ground, seems extraordinary. This is where the protection that certain rights must have, also at the international level, becomes effective. This is a criminal phenomenon that moves 10.5 trillion USD in profits worldwide and in which today more than 90 per cent of investigative activities depend on international forms of cooperation.

These investigative activities can take various forms, as described in detail by President Balsamo. There is "static" cooperation, such as the exchange of information supported by the Budapest Convention with the network of contact points, which has led to the freezing of distant sources of evidence around the world, but also, increasingly today, "dynamic" cooperation, fuelled by joint investigations, which take place within cooperation bodies and make use of often joint investigation teams.

Cooperation increasingly requires effective operational collaboration, through joint activities, because crime, especially the most serious forms of

50 Anglophone acronym equivalent to Least Developed Countries (NDR).

crime, such as child pornography and computer fraud on an international scale, have such a radically dimension transnational that investigations can only be shared between several states. This allows the international community to benefit in the prosecution and identification of perpetrators of large-scale crimes.

The international dimension is intrinsic to cybercrime. Much has been done in terms of international cooperation, especially in Europe, with tools such as the Joint Investigation Team and the European Investigation Order, which now allow us to talk about shared investigations, both at police and judiciary level, thanks to the coordination of Eurojust.

This is the terrain on which the international evolution of the fight against must move cybercrime, also at a non-European level: the creation of a legal framework common for the means of searching for evidence, the qualification of offences, the acquisition, exchange and validation of evidence, based on a common vision of concrete investigative tools and activities. This requires the emergence and evolution of international cooperation bodies and specialised police forces that can operate side by side, validating investigative activities in combating transnational phenomena.

This is the future to move towards. The UN Convention on Cybercrime is the starting point, the framework long-awaited; it will make it possible to be not only more effective, but also more efficient, by fostering economies of scale and the emergence of investigative teams that take advantage of a common legal culture.

Hannes Glantshnig
Vice President of the Cybercrime Team, Eurojust

Introduction: The Growing Threat of Cybercrime

Cybercrime is not a new phenomenon, but its scope, scale, and sophistication have grown exponentially in recent years. The digital revolution has brought about unprecedented opportunities for progress, innovation, and connectivity. However, it has also opened new frontiers for criminal activities that transcend national borders, exploit technological advancements, and challenge the very foundations of our legal and institutional frameworks. These challenges range from the overwhelming volume of data in investigations to the increasing use of anonymization and encryption by criminals. Each of these challenges poses significant obstacles to law enforcement and the judiciary, and addressing them requires both innovative solutions and enhanced international cooperation.

The Volume and Complexity of Data

One of the most pressing issues highlighted is the sheer volume of data involved in cybercrime investigations. Today, we are dealing with investigations that require the analysis of terabytes and even petabytes of data. The storage, management, and analysis of such vast amounts of information demand advanced technological tools, significant resources, and, crucially, the ability to cooperate seamlessly across jurisdictions. The management of large data volumes is not just a technical challenge but also a legal one. We must ensure that data is collected, stored, and analysed in ways that respect privacy and human rights while still enabling effective criminal investigations. This delicate balance is difficult to achieve, especially when legal frameworks vary widely between jurisdictions.

The fragmentation of data retention laws across Europe, exacerbated by the invalidation of the Data Retention Directive by the Court of Justice of the European Union, has created a patchwork of regulations that often lead to the loss of crucial data before it can be accessed by law enforcement.

Anonymization and Encryption: The Double-Edged Sword

Anonymization and encryption are critical tools for protecting privacy and securing communications in the digital age. However, these same tools are increasingly used by criminals to conceal their activities, making it extraordinarily difficult for law enforcement to trace and prosecute cybercriminals. The varied legal provisions across EU member states concerning access

to encrypted information add another layer of complexity to our efforts. For instance, while some countries have laws that compel the decryption of information under certain conditions, others have strong protections against such actions. This legal disparity not only complicates investigations but also creates safe havens for cybercriminals who can operate with impunity in jurisdictions with less stringent laws.

Operation Trojan Shield

In June 2021, Operation Trojan Shield was a large-scale, coordinated international law enforcement operation led by the FBI in collaboration with Eurojust, Europol and several other law enforcement agencies worldwide. The operation targeted global organized crime networks by exploiting the criminals' trust in an encrypted communication platform known as ANOM. ANOM was a secure messaging app secretly developed and controlled by the FBI. The app was designed to mimic other encrypted messaging services frequently used by criminals, but it had a crucial difference: it allowed law enforcement to monitor all communications in real-time. The platform was distributed to criminal networks through undercover agents and informants, gaining credibility among high-level criminal organizations involved in drug trafficking, money laundering, and other illicit activities. Over three years, more than 27 million messages were intercepted from 12,000 devices across over 100 countries. These messages provided invaluable intelligence about criminal operations, including planned drug shipments, money laundering activities, and violent assaults. The data gathered from ANOM allowed law enforcement agencies to carry out numerous raids and arrests around the world.

The operation resulted in the arrest of over 800 individuals globally, the seizure of more than 8 tons of cocaine, 22 tons of cannabis, 2 tons of synthetic drugs, 250 firearms, 55 luxury vehicles, and over $48 million in cash and cryptocurrencies. These actions struck a significant blow to organized crime by disrupting various criminal enterprises and networks. Operation Trojan Shield showcased the power of international collaboration and innovative law enforcement strategies in addressing the complexities of modern organized crime. By using a covert platform, law enforcement agencies demonstrated that leveraging technology could effectively infiltrate and dismantle criminal networks operating across borders. This operation serves as an example of how smooth and fast cooperation between law enforcement agencies worldwide, coupled with advanced technological tactics, can significantly impact global crime.

International Cooperation: A Necessity, Not a Choice

The transnational nature of cybercrime makes international cooperation not just desirable but essential. However, achieving effective cooperation is easier said than done. Legal and logistical barriers often impede the flow of information and evidence between countries, slowing down investigations and allowing criminals to exploit jurisdictional gaps. The SIRIUS Project by Eurojust and Europol, which fosters cooperation in serious crime investigations, is an excellent example of how international collaboration can be effective. Through extensive training programs, the sharing of best practices, and comprehensive reporting, the project has made significant strides in enhancing cross-border cooperation. However, these efforts must be supported by robust, harmonized legislative frameworks that facilitate, rather than hinder, international cooperation. The introduction of new EU legislative tools, such as the e-evidence Package and the Digital Services Act, represents significant progress. These frameworks aim to streamline processes and enhance the ability of competent authorities to manage large data sets, enforce regulations, and foster international cooperation. Yet, the true measure of their effectiveness will be in their practical application and the extent to which they can be integrated into existing strategies across member states and beyond.

Artificial Intelligence: The Next Frontier

As we look to the future, the regulation of Artificial Intelligence (AI) on a global level will be crucial. AI holds immense potential to both combat and facilitate cybercrime, making it a double-edged sword that requires careful handling. The European Union's Artificial Intelligence Act is a commendable step in the right direction, aiming to create a robust regulatory framework that addresses the ethical and safety implications of AI. However, AI is not confined by national borders, and its regulation will require a concerted global effort. The integration of AI into cybercriminal activities adds another layer of complexity to an already challenging landscape. AI can be used to automate and scale cyberattacks, making them more efficient and harder to detect. For instance, AI-driven malware can learn from its environment and adapt its behaviour to avoid detection by traditional security measures. This creates an urgent need for new strategies and tools to combat AI-enhanced cybercrime. At the same time, AI can be a powerful tool for law enforcement. Advanced AI algorithms can sift through vast amounts of data to identify patterns, predict criminal behaviour, and even simulate potential outcomes of different law enforcement strategies. However, the use of AI in law enforcement also raises important ethical and legal questions. How do we ensure that AI sys-

tems are transparent, accountable, and free from bias? How do we balance the need for security with the protection of individual rights?

The Disturbing Rise of AI-Generated Child Sexual Abuse Material

Another deeply concerning development in the realm of cybercrime is the increasing use of Artificial Intelligence (AI) to create child sexual abuse material (CSAM). Over the past few years, we have witnessed a dramatic rise in both the quantity and quality of AI-generated CSAM, posing unprecedented challenges for law enforcement, the judiciary, and society at large. AI has the capability to generate highly realistic images and videos of child abuse, blurring the lines between real and fabricated content. This creates significant difficulties for investigators who must distinguish between genuine cases of abuse and AI-generated material. The process of verifying the authenticity of this content is not only time-consuming but also mentally and emotionally taxing for those involved in the investigations. Moreover, the existence of such realistic fake material complicates the legal processes, potentially leading to issues in prosecution and justice for victims.

However, the damage caused by AI-generated CSAM extends far beyond the digital realm. Perpetrators often use images of real children—sometimes children in their own vicinity—as the basis for these AI-generated materials. This not only puts these children at direct risk but also perpetuates a cycle of abuse, where the consumption of such material fuels the demand for more extreme and explicit content. The very existence of AI-generated CSAM can encourage perpetrators to commit further crimes, including the grooming and abduction of actual victims. The situation is exacerbated by the emergence of malicious AI-driven chatbots that actively antagonize suspects into committing crimes. These chatbots can engage potential offenders with explicit content, including images and voice messages, and even provide detailed guides on grooming, abducting victims, and evading detection. These AI tools are designed to exploit the vulnerabilities of individuals, pushing them further down the path of criminal behaviour and making them more dangerous to society. The rise of AI-generated CSAM and the use of malicious AI-driven chatbots represent a new and terrifying frontier in cybercrime. They highlight the need for a multi-faceted response that includes technological solutions, robust legal frameworks, and enhanced international cooperation. Law enforcement agencies must be equipped with the latest AI detection tools and trained to deal with these new forms of criminality. At the same time, there must be stricter regulations governing the development and use of AI technologies to prevent their exploitation by criminal elements. This

is not just a challenge for law enforcement; it is a moral imperative for society as a whole. The exploitation of children, whether through AI-generated materials or other means, is one of the most heinous crimes imaginable. We must work together, across borders and disciplines, to protect the most vulnerable members of our society from the dangers posed by these emerging technologies.

Example for Use of AI by Law Enforcement

To illustrate the potential of advanced AI techniques in modern law enforcement, consider the approach taken by one European country in tackling the heinous crime of child sexual abuse material (CSAM) circulating online. Law enforcement agencies in this country have integrated voice recognition technology to identify suspects speaking in the national language within illicit videos. This innovative approach begins with the collection of CSAM from various online platforms. The content is then processed using sophisticated AI algorithms capable of recognizing different languages. But the process doesn't stop there. The video is further analysed using AI-driven facial recognition technology. Both victims and suspects' faces are identified and then cross-referenced with the national passport and prison databases. This multi-layered AI approach allows for an extensive comparison against official records, leading to the precise identification of suspects and potential rescue of victims.

The impact of this technology is profound. Last year alone, over 200 suspects were identified using this combined AI and voice recognition technique. To put this into perspective, law enforcement agencies estimate that without these advanced tools, only about six suspects would have been identified using traditional methods. This example underscores the power of integrating AI into law enforcement's toolkit. It highlights the urgent need for international cooperation, technological advancements, and robust legal frameworks to support such innovative approaches in combating the ever-evolving landscape of cybercrime.

The Rise of Fake Websites: A New Facet of Cybercrime

In recent years, we have witnessed a sharp increase in the use of fake websites as tools for cybercrime. These websites, which often mimic legitimate businesses, financial institutions, or government agencies, are designed to deceive users into providing personal information, downloading malware, or making fraudulent payments. The sophistication of these fake websites is alarming—they often feature realistic designs, secure-looking URLs, and even fake customer service interactions to enhance their credibility.

The proliferation of fake websites represents a significant challenge for both law enforcement and the judiciary. The anonymity of the internet makes it easy for cybercriminals to create and operate these sites from anywhere in the world, often using hosting services in jurisdictions with weak enforcement mechanisms. Once these sites are identified and taken down, they can quickly reappear under a different name or URL, making it a never-ending game of cat and mouse for authorities.

Moreover, the impact of fake websites extends beyond financial losses for victims. These sites erode trust in digital services, making people wary of conducting legitimate online

The Role of Criminal Jurisdiction in Virtual Space

As we deal with these challenges, one of the central issues we must address is the role of criminal jurisdiction in virtual space. Cybercrime is inherently transnational, often involving perpetrators, victims, and evidence spread across multiple jurisdictions. Traditional notions of jurisdiction, based on territoriality, are increasingly inadequate in this context. The InterPlanetary File System (IPFS) for example is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. It represents a significant departure from the traditional centralized web architecture, offering unique advantages in terms of data distribution, resilience, and censorship resistance. However, IPFS also presents significant challenges for law enforcement, particularly in cybercrime investigations. Unlike the traditional HTTP protocol, which relies on centralized servers, IPFS operates on a decentralized network of nodes. Each node stores a part of the overall data, and content is retrieved using a content-based addressing system rather than a location-based one. This means that files are accessed based on their cryptographic hash as unique identifier, not their location on a specific server. IPFS is a P2P protocol, meaning it connects users directly to share files. When a user requests a file, the network retrieves it from the nearest or fastest node hosting the file or parts of it, rather than a single centralized server. This allows for faster file retrieval and reduced bandwidth costs.

By design, IPFS is highly resistant to censorship and data loss. Since data is distributed across numerous nodes globally, taking down a specific piece of content becomes almost impossible without shutting down the entire network. This makes IPFS attractive for users who seek resilience against data censorship, such as activists or developers in regions with restrictive internet policies. Due to the global nature of IPFS, illegal content may be hosted across multiple jurisdictions, making it difficult to apply national laws ef-

fectively. Even if some nodes are located in a country where specific content is illegal, other nodes may exist in countries where the same content is not regulated, creating a jurisdictional grey area. The effectiveness of criminal jurisdiction in virtual space is contingent on several factors, including the ability to attribute cybercrimes to specific actors, the willingness of states to cooperate, and the availability of legal tools that can be effectively applied in a digital environment. The ongoing discussions at the United Nations, particularly the work of the Open-Ended Working Group on Cybercrime and the preparatory work for the UNODC Convention on Cybercrime, are crucial in this regard.

These discussions are not just academic exercises; they have real-world implications for how we respond to cybercrime. The UNODC Convention on Cybercrime aims to contribute to more adequate definitions of cybercrimes and to universalize the principles of judicial cooperation in criminal matters, as set out in the Budapest Convention and its Second Additional Protocol. However, for these efforts to be successful, they must be informed by the realities of cybercrime and the unique challenges posed by virtual space.

Cybersecurity and National Sovereignty

Cybercrime is not just a criminal issue; it is also a matter of national security and sovereignty. A cyberattack on critical infrastructure, for example, can have devastating consequences for a nation's security, economy, and public safety. Such attacks require a coordinated response that involves not just law enforcement but also intelligence agencies, cybersecurity experts, and, in some cases, the military. The concept of sovereignty in cyberspace is still evolving, and there is a need for clearer rules and norms to govern state behaviour in this domain. The Tallinn Manuals, for instance, provide valuable guidance on how international law applies to cyber operations, but more work is needed to develop a comprehensive legal framework that can be universally applied.

The Importance of a Comprehensive Approach

The challenges we face in combating cybercrime are complex and multifaceted, and they require a comprehensive approach that goes beyond traditional law enforcement methods. We must leverage the expertise of legal scholars, technologists, and policymakers to develop innovative solutions that can keep pace with the rapidly evolving threat landscape. One of the key takeaways from my experience as a prosecutor working in cybercrime cases for over a decade and now at Eurojust is the need for greater integration of law enforcement and judicial efforts across borders. This integration must be

supported by a strong legal framework that facilitates cooperation, enables the sharing of information and evidence in real time, and ensures that cybercriminals cannot exploit jurisdictional gaps to evade justice. At the same time, we must also look to the future and anticipate the challenges that will arise as new technologies, such as quantum computing, become more widely adopted. Quantum computing has the potential to revolutionize many areas of science and technology, but it also poses significant risks to cybersecurity. The ability of quantum computers to break current encryption methods could render many of our existing security measures obsolete, creating new opportunities for cybercriminals.

Conclusion

In conclusion, the fight against cybercrime is not just a legal or technical challenge; it is a global challenge that requires a coordinated and sustained effort from all of us. We must continue to build on the progress we have made, address the gaps and weaknesses in our current systems, and work together to create a safer, more secure digital world. The smooth and efficient cooperation between law enforcement agencies and the judiciary is essential to this effort. By harmonizing our legal frameworks, enhancing international cooperation, and regulating emerging technologies like AI, we can better protect our societies from the ever-present threat of cybercrime.

Let us take this opportunity to reaffirm our commitment to this cause and to work together to build a future where the rule of law prevails in cyberspace, just as it does in the physical world.

Edvardas Sileris
Head of the European Cybercrime Centre, Europol

Good morning, distinguished guests, colleagues, and partners,

It is a pleasure to address you today on the critical and timely topic of cyberspace, cybercrime, and the importance of effective international cooperation. The cyber landscape continues to evolve rapidly, presenting challenges that require innovative, agile responses. The threats we face are more sophisticated than ever before, and the scale of these challenges demands that we work together — across borders, sectors, and disciplines. In today's interconnected world, cybercriminals exploit the very technologies that enable our societies to thrive. From ransomware attacks to phishing schemes and e-commerce fraud, these activities are often transnational, necessitating a global response. This is where multilateral police and judicial cooperation, such as that coordinated by Europol and other key institutions, becomes indispensable.

Adapting to Evolving Threats

One of the central themes in our fight against cybercrime is adaptability. The criminal ecosystem has evolved significantly, influenced by technological advances and geopolitical shifts. In this dynamic environment, our ability to swiftly coordinate with a wide array of actors is crucial. This is why police cooperation, is critical. With European partners and also with some other international actors, the Europol Cybercrime Centre (EC3) has developed an extensive network, in supporting operations. Such networks not only facilitate information sharing but also contribute to the development of comprehensive threat assessments, which guide our strategies in addressing cybercrime.

The UN Convention on Cybercrime offers an important starting framework for judicial cooperation, but it also addresses key aspects of police collaboration. In particular, the Convention enhances international cooperation by establishing shared principles for criminalization and jurisdiction. It also introduces specific measures for law enforcement, we specifically consider those on general principles of cooperation, the 24/7 contact points, and on law enforcement cooperation and joint investigations.

These 24/7 contact points are essential players in the global fight against cybercrime. Their role in processing requests and exchanging information across different networks — whether it's the G7, Budapest Convention, INTERPOL or Europol's SIENA system — cannot be overstated. By fostering

this real-time exchange of information, we improve our ability to respond to cyber threats rapidly and effectively.

Leveraging the UN Convention for New Challenges

The UN Convention provides us with a framework to strengthen law enforcement capabilities, particularly in reaching countries worldwide. This is critical in our fight against emerging forms of cybercrime, such as ransomware, where cross-border cooperation is essential. One of the ongoing challenges in cybercrime investigations, such as those involving ransomware, is the need for law enforcement agencies to access criminal servers in foreign jurisdictions. As we've seen in recent cases, these servers are often located outside trusted jurisdictions, creating significant difficulties for agencies trying to intervene. The UN Convention can help mitigate these challenges by fostering greater cooperation and facilitating the sharing of evidence across borders.

Additionally, the Convention provides new opportunities to engage with countries where cybercrime activities, such as sextortion, and e-commerce fraud, are prevalent. In regions like Western Africa and parts of Asia, cooperation is critical to identifying offenders and mitigating criminal activities like romance scams and child exploitation.

The growing threat of AI-driven crime also demands our attention. As artificial intelligence becomes more accessible to criminals, its potential to increase the sophistication and scale of cybercrime is alarming. From deepfakes used in fraud and identity theft to AI tools deployed in social engineering attacks, we must prepare for this new frontier. The UN Convention offers a starting point to develop safeguards against these AI-driven threats, particularly in cases of deepfake impersonation or the production of child sexual abuse material.

Building on Best Practices

Europol has long been a laboratory for best practices in police cooperation, continually adapting to new threats. The European Cybercrime Centre (EC3), for instance, has introduced innovative approaches to operational coordination, as seen in its Joint Cybercrime Action Taskforce (JCAT) and initiatives like the Internet Referral Unit (IRU). These efforts have led to significant successes in mitigating the impact of large-scale cyber threats, including ransomware and Darknet platforms like Raidforum.

Public-private partnerships are another cornerstone of our success. By collaborating with industry actors and other stakeholders, Europol has been

able to provide global solutions for victims and operational actors alike. Operations like EMOTET remediation and takedown actions such as PowerOff demonstrate the effectiveness of these partnerships in neutralizing criminal infrastructures. However, beyond the UN Convention, major challenges will still need to be solved. Legal frameworks are just one part of the solution. Access to data, particularly transborder access, remains a significant hurdle for law enforcement. The ability to retrieve evidence from cloud providers or servers located in foreign jurisdictions often depends on a patchwork of legal, standards and cooperation agreements. To overcome these obstacles, we need to ensure that cooperation extends beyond law enforcement to include the private sector and other communities. Future successes in fighting cybercrime will hinge on our ability to create synergy between these various stakeholders, establish friendly technological standards, and promote proactive information-sharing practices.

Looking Ahead: Promising Results and the Road Forward

Already, we are seeing the results of enhanced police cooperation in the fight against cybercrime. Recent operations supported by Europol at the international and EU levels have been emblematic of what can be achieved when we work together. For example, coordinated efforts have led to the dismantling of organized cybercrime groups, disrupted key criminal infrastructures, and even taken down major Darknet platforms. However, more can be done. As we look toward the future, we must continue to build on these successes. The UN Convention on Cybercrime is a promising tool, but its true potential will only be realized if we can address the remaining challenges—namely, easing law enforcement access to data and fostering greater international cooperation across all sectors.

In conclusion, cybercrime is a global threat that requires a global response. With the right legal frameworks, operational coordination, and cooperation across borders, we can significantly reduce the impact of cybercrime and protect our societies from these ever-evolving threats. Let us continue to innovate, collaborate, and build the capacities we need to ensure a safer digital world for all.

Thank you.

DEBATE

Eugenio Albamonte:

I would like to highlight some of the stimuli that have emerged from the speeches I have just heard, such as the prospects for implementation, the increased joint operation of the investigative actors in the field, the sharing of new technologies applied to investigations, and this to ensure that all institutions - police forces and judicial authorities - have a homogeneous capacity for action in the cyber environment; and again, the homogenisation of approach, which must not only concern the regime of storage and access to computer data, but also the standards used by the different police forces for data collection and analysis. It is also important to ensure the effectiveness of information exchange and active police action in cyberspace, not only in a reactive but also a preventive manner. What comes into play here, in other words, is not only investigations aimed at detecting and prosecuting offenders, but also the preventive function of law enforcement agencies. In this sense, once inevitably malicious infrastructures have been identified, it would be necessary to be able to intervene on them before they are used to commit crimes.

I would like to offer a further food for thought.

It relates to the important impetus given by Article 32 of the Budapest Convention on Cybercrime, which enabled direct, informal and unstructured cooperation between the public and the private sector, i.e. between the state, police forces, prosecutors and Internet Service Providers, in the acquisition and collection of data that are essential for the rapid identification of subjects.

Article 32 also has another scope, allowing the use of the network to carry out investigations through cyberspace, even in places that could be removed from state jurisdiction. It is thanks to this instrument that, several years ago, as a public prosecutor in the context of an investigation into computer crime, I was able to carry out a computer inspection on foreign servers, operated from Italy, to check whether certain Google servers were hosting criminal content. These are spontaneous, very informal forms of cooperation, which, however, considerably increase the dimension, operativeness and timeliness of our actions.

If this positive experience in the relationship between public and private actors could be extended to relationships between public actors, between states, between judicial authorities and judicial police forces, it would be an important step forward.

Ivano Gabrielli:

In picking up on this last cue, I would like to point out that as law enforcement authorities we have over time increasingly benefited from voluntary cooperation, with multiple actors operating across geographical and political boundaries, providing services and managing clientele beyond national borders. These actors have adhered to public-private cooperation models that have proven to be very productive and profitable. Unfortunately, alongside these positive models, we have also experienced situations in which access to legitimate operations has been systematically denied, resulting in clear and recognisable areas of illegality.

Today, a quantum leap is needed. The universality of an instrument such as a UN Convention on cybercrime allows us to look at modes of cooperation that are no longer based solely on voluntary membership, but legitimise forms of cooperation between states. In short, we must find forms of cooperation that go beyond the model based on "freezing" and subsequent data acquisition, moving towards active and dynamic cooperation, cooperation that necessarily also requires mutual recognition of investigative tools.

The speed with which cybercrime moves across borders poses the need to be quick in searching for evidence, including through effective investigative tools such as those already in use in the fight against child pornography and more aggressive forms of cybercrime. This refers to undercover activities, which often move into undefined virtual spaces that cannot be allocated geographically and therefore cannot be easily traced to the jurisdiction of a single state.

Cyberspace is a shared space where both legitimate and criminal economies move extremely fast. Criminal organisations have significant resources, are familiar with legislation and are able to adapt their activities to international regulatory changes and the reaction capabilities of certain countries.

It is crucial, therefore, to have a fast cooperation, which passes through a preliminary recognition of the capacities to acquire evidence, evidence that can then be validated by the judicial authorities. In other words, we need to move towards an approach aimed at making better use of the operational capacity of the various countries, firstly allowing the respective police forces to participate in joint investigative activities, acting quickly when the seriousness of a crime warrants it, and then having the evidence obtained validated by the judicial authorities.

This becomes essential, for example, to counter phenomena such as the production, sale and dissemination of child pornography. In my opinion, we must be able to act even remotely, carrying out investigative activities with

speed, making proactive efforts to counter such multifaceted forms of crime, fast and adaptable to the international legal landscape and framework.

Hannes Glantschnig:

I too would like to emphasise that speed in investigations is a fundamental value, as stated in an article of the Budapest Convention on Cybercrime.

Upstream, however, much of the information we share at police level with Europol and Interpol creates a usability problem for the prosecution, as this information is often in nature *intelligence* and therefore cannot be used in the trial. As a result, arrest warrants often cannot be obtained precisely because the source would be data *intelligence*. It is therefore necessary to create the conditions for the issuing of orders or warrants at European level so that this information can be used as evidence in court.

Returning to the "speed" factor, efforts have certainly been made to speed up processes, but we are still at the stage where we have to print, sign and send documents by traditional means. Sometimes we even send faxes, a mode that is no longer common in many countries, but a new system is being worked on to send information electronically to ensure it is sent and received quickly. However, the problem of time for language translations remains. In the future, we may have automatic translation, but if today a criminal opens an account in every European country and transfers funds from one account to another, following them up with a traditional method may take too long to yield profitable results.

There is, however, the possibility of circumventing the slowness of such a procedure through the *spontaneous* exchange of information: through Eurojust, information can be exchanged without the need for translation into the other's national language, and this information can be shared with any country[51]; this is a very convenient and useful mechanism that should be better known and exploited.

---

51 We refer to Art. 21 of EU Regulation 2018/1727 establishing and regulating the EUROJUST Agency, entitled "Exchange of information with Member States and between national members", which provides, inter alia, that the competent authorities of the Member States shall exchange with Eurojust all information necessary for the performance of its tasks, ...including information on the setting up of joint investigation teams, cases in which forms of mutual legal assistance have been set up with at least two Member States; and that the national members themselves exchange with each other or with the competent national authorities, without prior authorisation, all the information necessary for the performance of Eurojust's tasks. In particular, the competent national authorities shall inform their national members without delay of cases concerning them [Ed.]

And again, speed is *provider information management*, but also essentialis crucial.

Often in investigations, one is confronted with service providers one has never met before, who are not even named; one does not know what kind of data it keeps, where it can be obtained and how long it will be kept. Moreover, it is not clear what kind of information is required to access this data. For most providers, we have information on what and to which address to send, and for how long the requested information will be available. If you want information from a provider, there is a structured procedure to follow and you do not have to search for the information on their homepage. This is a very important profile that needs to be known.

As a Eurojust agency, we also carry out training and develop fact sheets. If you need, for example, to send a request for judicial assistance to Japan, you can find a ready-made request format.

Edvardas Sileris:

Speaking of bottlenecks, it should be pointed out that sometimes, for instance, police forces cannot act effectively because data are privately owned. In order to address and overcome this impasse, in Europol's Cybercrime Centre we have set up advisory groups to also acquire the know-how of private entities. So far, we have been successful and efficient, increasingly including private individuals in our activities. But sometimes difficulties remain.

Let me give you the example of ransomware attacks, where this criticality is frequently experienced: usually, when there is a victim of a ransomware attack, those who react are the private sector, not the police, because the latter do not know how to help the victim. In other words, we law enforcement authorities know that there is an attack in progress, but we do not know the infrastructure or the software that is carrying out the attack. This means that it is the cybersecurity companies that intervene to solve the problem for the attacked company. We also do not have unified protocols on how to collect data of interest from the private sector in order to get to the control centre of the attack. Therefore, as mentioned, it is the private sector that reacts first and then, only eventually, the police intervene.

We need to understand how to deal with the problem and what can be useful for criminal investigation, because in many cases it does not take long. Private individuals should collect data with new IP addresses, data that in turn could contain information of great value to investigators. Links to a criminal group, responsible for the attack, could be identified from this and from there lead to arrests in the future.

My message is therefore that private partners are crucial and we have to find the best ways to get information efficiently from them and reduce the bureaucratic burden of our way of doing things as much as possible.

THIRD SESSION

EFFECTIVE JURISDICTION IN TRANSNATIONAL CYBERCRIMES. CONVENTIONS IN ACT AND IN PROGRESS

EFFECTIVE JURISDICTION IN TRANSNATIONAL CYBERCRIMES. CONVENTIONS IN ACT AND IN PROGRESS

CHAIRPERSON

Luigi Salvato
Attorney General of the Court of Cassation

In opening this last session, for the time and task entrusted to me, I will limit myself to observing that the technological revolution must be governed with effective and efficient rules, a feature also guaranteed by the jurisdiction, which is being challenged by cyberspace.

Jurisdiction is in fact an expression of sovereignty, the main attribute of states. A cornerstone of international law is the customary rule of territorial sovereignty: the state enjoys exclusive jurisdiction within its territory and any unauthorised exercise of power in another's territory is unlawful under international law.

However, space-time boundaries have been crumbled by cyberspace. Its characteristic feature is its a-territoriality, enhanced by the condition of anonymity, guaranteed by the use of cryptographic solutions, the cause of the so-called *loss of location*, which makes it complicated to establish the "who", "how" and "where" of a cyber-criminal action. In cyberspace, national states also seem to lose strength to large corporations that manage transnational infrastructures, made up of various segments, which escape territorialisation, a constituent element of sovereignty and a primary aspect of the exercise of jurisdiction and law regulating relations between states.

Yet, virtual space is still a material space attached to the territory. Any computer data must ultimately be stored on a physical medium. Considering that an offence is committed in the State, when the action or omission, or at least a part of the conduct or event, has taken place in the national territory - according to a rule established in the Italian legal system by Article 6 of the CodePenal . - the question is that of the actions that make it effective. It is these that come into collision with the sovereignty of other states, with other jurisdictions, and make a defence by means of cybersecurity structures established within individual states complicated.

The transnational nature of cybercrime has demonstrated the inadequacy of the rogatory instrument, a traditional instrument of dialogue in international law, but between states, not between judicial authorities, which ensures

control within its own sovereign sphere, but does not provide certainty in the response, does not guarantee agility and speed in execution.

Cyberspace requires the rethinking of traditional legal institutions, an aim that supports the topicality of the thought and activity of Vittorio Occorsio, in whose name the Foundation organising the event that brings us together operates. As Giovanni Salvi wrote, Vittorio Occorsio had arrived at important results "because he had not acquiesced in the use of current interpretative categories" and "had operated, together with other colleagues, in an innovative manner".

The ability to adapt and innovate legal institutions must meet the challenges posed by the scientific revolution.

The aim is to give effectiveness to the rule, of which jurisdiction is an irreplaceable safeguard and which, by securing it through the process, guarantees fundamental rights, without discrimination, and the reasonable balancing of the same with the duties established by criminal law.

The international community, albeit with known difficulties, is developing responses inspired by this conviction, through the evolution of judicial cooperation instruments, which has taken place within the Council of Europe, the European Union and the UN.

Today's speeches will take stock of this development, of strategies that can guarantee the effectiveness of jurisdiction, but also of investigation strategies that have an autonomous task, as a preventive security guard, and a concurrent one, as they are part of the process.

COUNTERMEASURES UNDER INTERNATIONAL LAW IN RESPONSE TO CYBER OPERATIONS FROM OTHER STATES

Marco Roscini
Professor of International Law at the University of Westminster (London), Professor of International Humanitarian Law at the Geneva Academy of International Humanitarian Law and Human Rights

Picture this very frequent scenario: malicious cyber operations are conducted against Italy and/or Italian companies from another state, for instance to disrupt the functioning of wired infrastructure or to acquire industrial secrets. We do not know with any certainty who is responsible for them, all we know is that they originate from cyber infrastructure located in that foreign state. What I would like to talk about is whether international law allows the victim state to address the problem at its root, that is, by taking direct action on the territory of the state where the cyber threat originates from. This action would constitute an exercise of extraterritorial enforcement jurisdiction. Extraterritorial enforcement jurisdiction in cyberspace can be exercised to access and extract data stored on foreign servers or computers in order to collect evidence necessary to establish the responsibility of a state or for use in criminal proceedings. Extraterritorial enforcement jurisdiction can also take the form of hack-backs to shut down the foreign servers used to conduct the operations or to disinfect bots.

Does international law allow the exercise of extraterritorial jurisdiction? Several rules of international law come into play in this context, the main ones being the rule protecting territorial sovereignty and the principle of non-intervention in the domestic affairs of other states. It is not surprising that Article 5 of the draft UN Cybercrime Convention reaffirms both and cautions that, as a rule, nothing in the Convention entitles states to exercise jurisdiction and perform functions on the territory of other states.

Starting from the rule protecting territorial sovereignty, sovereignty is a foundational principle of international law, which – at least since the Peace of Westphalia of 1648 – has a strictly territorial connotation: the international order is organised around a multitude of states, which can exercise sovereign authority over a portion of the earth's surface to the exclusion of other states. This authority is exactly what we call "jurisdiction" and is normally exercised by a state over individuals, objects, and events within its territory. Jurisdiction can consist in the enaction, modification and revocation of binding regula-

tions (prescriptive jurisdiction), the implementation of these binding regulations (enforcement jurisdiction), and the settlement of disputes arising from them (judicial jurisdiction). As already said, investigative searches and hack-backs are an example of enforcement jurisdiction.

What international law says in regard to the extraterritorial exercise of jurisdiction is still essentially contained in the classic 1927 *Lotus* judgment of the Permanent Court of International Justice, where the Court distinguishes the exercise of enforcement jurisdiction from other forms of jurisdiction. While a state cannot exercise "its power in any form" (that is, enforcement jurisdiction) in the territory of another state without its consent or a permissive rule of international law, it can "extend the application of [its] laws and the jurisdiction of [its] courts to persons, property and acts outside [its] territory" unless there is a prohibitive rule of international law. So the exercise of extraterritorial enforcement jurisdiction is prohibited unless it is permitted, while the exercise of extraterritorial prescriptive/judicial jurisdiction is permitted unless it is prohibited. The reason for the different treatment is that the extraterritorial exercise of enforcement jurisdiction is a far more intrusive exercise of authority on the territory of the target state than the adoption of laws and judicial acts. The overeach of prescriptive jurisdiction and the rigid territorial approach of enforcement jurisdiction can create an enforcement gap which is particularly evident in the virtual space.[52]

In order not to breach the territorial sovereignty of the target state, therefore, the enforcing state will need a legal basis for the cross-border hack-back or investigative search: indeed, even if data are stored "in the cloud", they still exist in one or more physical servers located in the territory of some state. This legal basis can be the consent of the competent authority of the territorial state granted after an ad hoc request. Alternatively (or in addition), the legal basis can be a treaty in force between all concerned states which allows a state party's authorities to hack-back or conduct investigative searches in the cyber infrastructure of another state party even without securing its ad hoc consent first. A middle ground is Article 32 of the Budapest Convention on Cybercrime, which provides that a party can access or receive stored computer data located in another party without its authorisation but only if it has the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system. Ultimately, however, states must rely on state consent and, thus, on international cooperation and mutual

52 Kohl, 76. The US Cloud Act extends US jurisdiction over all data controlled by local platforms regardless of their location. This allows to bridge the enforcement gap between the overreach of prescriptive jurisdiction and the rigid territorial approach of enforcement jurisdiction.

legal assistance treaties to enforce their laws extraterritorially, and cyberspace is no exception.

More flexible approaches to extraterritorial investigative searches in cyberspace which apply the more permissive rules of prescriptive jurisdiction remain essentially the position of the Western states and are resisted by states that want to maintain a strong control over their cyberspace and thus consider digital evidence like any other evidence. No customary exception to the *Lotus* principle has thus formed for extraterritorial investigative searches in cyberspace just yet, and this is even more true for hack-backs aimed at shutting down servers abroad.[53]

Not only would cross-border enforcement actions in cyberspace without a legal basis or a permissive rule of international law be a violation of the territorial sovereignty of the target state, they would also be a violation of the principle of non-intervention. This principle is one of the oldest rules of international law as it is a corollary of state sovereignty. It protects states from any coercive acts in their internal affairs, that is, it prohibits states to coerce other states into doing something they have the right not to do and into not doing something they have the right to do. Hack-backs and non-consensual extraterritorial investigative searches are coercive in that, they impose a condition of things (server shutdown, exfiltration of non-public information stored on their territory) on the target state.

So the extraterritorial exercise of enforcement jurisdiction by hacking back is prohibited by at least two rules of international law. Does this mean that there is nothing we can do to stop the malicious cyber operations originating from abroad or to collect evidence about them when this evidence is stored in computers and servers abroad and the territorial state refuses to cooperate? In the absence of a permissive legal basis, our extraterritorial response will be illegal under international law but this illegality could be precluded by the fact that it is taken against a previous wrongful act committed against us by another state. This is the doctrine of countermeasures, which has a solid basis under customary international law as also confirmed in the Italian position paper on the application of international law in cyberspace.

---

53 Netherlands 2019: 'The act of exercising investigative powers in a cross-border context is traditionally deemed a violation of a country's sovereignty unless the country in question has explicitly granted permission … Opinion is divided as to what qualifies as exercising investigative powers in a cross-border context and when it is permissible without a legal basis founded in a treaty. In cyberspace too, countries' practices differ in their practical approaches to the principle of sovereignty in relation to criminal investigations'. AU Common Position: 'enforcement authority on the territory of a foreign State … even if the exercise of such enforcement authority by a State does not have harmful effects, whether virtual or physical, on the territory of a foreign State'.

Countermeasures are a law-enforcement mechanism: you breach international law obligations towards me, I breach international law obligations towards you in order to implement your responsibility as the wrongdoing state. This is in fact how most international law is enforced. The main problem with using the doctrine of countermeasures to justify hack-backs or non-authorised extraterritorial investigative searches is that it requires a previous wrongful act committed by another state. In most cases, however, the malicious operations will be conducted by criminal groups without state involvement. Even if a state is responsible for them, it will likely be difficult to prove its responsibility with "a sufficient level of confidence" (to use the language of the Italian position paper on the application of international law in cyberspace).

In cases where the state from which the cyber operations originate is not, or cannot be proved to be, responsible for them, I argue that we might still justify the extraterritorial exercise of enforcement jurisdiction on its territory on the basis of the doctrine of countermeasures if we take the due diligence rule into account. This international law rule requires states to prevent that their territory is used for the commission of acts contrary to the rights of other states. For the violation of this rule, the territorial state needs 1) to have knowledge of the cyber operations against other states occurring from its territory; and 2) must have failed to take all feasible measures to terminate them. Due diligence allows us to circumvent the technical difficulties associated with attribution in the virtual space, as attribution of the cyber operations to a state is not needed – but it is responsibility for a *failure to act*, rather than liability for the act itself. Our hack-back to shut down servers would thus be a response to the territorial state's failure to adopt all feasible measures to terminate the cyber operations against us from those servers. In case of an investigative search, the evidence that we aim to obtain must be needed to stop the malicious operations that the territorial state is unwilling to terminate and/or to prevent their repetition. This argument, however, presents two potential weaknesses. First, not all states believe that due diligence is an actual binding rule of international law and prefer to see it as a mere norm of responsible behaviour – as something states should, not must, do: as such, states would not breach international law if they do not comply with it and there would be no wrongful act to respond to with countermeasures. However, a majority of states, including Italy,[54] consider due diligence to be a binding rule although it is unclear how much harm needs to be caused for this rule to be breached. Second, historically countermeasures have been construed as state-to-state measures, that is, they must be adopted by the injured state and directed

54 Italy's position paper in 'International Law and Cyberspace', 6.

against the responsible state in order to induce it to comply with the breached obligation: when the malicious cyber operations are conducted by criminal groups from abroad without the involvement of the territorial state, one could say that shutting down the servers they use or accessing non-public data to prosecute them is a reaction against the criminal group itself, and not the territorial state. This view, however, is not persuasive. Even though the criminal group would be the ultimate target of our response, it is the right of the state from where they operate that is breached by the cross-border enforcement action (namely, its territorial sovereignty and its right not to be coerced under the principle of non-intervention). So, the measures are taken "against" the territorial state. Furthermore, the law can change, and perhaps is undergoing change, in order to address the new realities of the virtual space. If the traditional understanding of countermeasures is that they are about inducing the wrongdoing state into legal compliance, a more modern approach is that they can also replace or supplement what the state should be doing as a matter of international law – countermeasures, in other words, are about *implementing state responsibility for breaches of international law*, including due diligence, *either* by compelling the responsible state to restore the legal status quo *or* by allowing the injured state to do so itself. This is a broadening of the traditional understanding of the doctrine of countermeasures which might be necessitated by the characteristics of the virtual space, including the attribution challenges and the prominent role played by non-state actors. In my view, this broadening still fits the countermeasures' rationale, that of implementing state responsibility. It goes without saying that all the requirements under the law of countermeasures must be complied with, in particular the effects of our response must be reversible where possible and must be proportionate to the injury suffered. In case of countermeasures in response to a due diligence breach, proportionality will need to be assessed in relation to the territorial state's omission to adopt all feasible measures to terminate the cyber operations from its territory, and not to the consequences of the cyber operations by criminal groups that the territorial state did not terminate.[55]

To conclude. Even though the extraterritorial exercise of enforcement jurisdiction in the virtual space is still unlawful under customary international law, in the same way as it is unlawful in the analogue world, this illegality can in certain circumstances be excluded by the fact that cross-border enforcement can be construed as a countermeasure against a previous wrongful act committed by the state where the cyber operations against us originates from, either because that state is responsible for them or because it has

55 Tallinn Manual, 130.

breached its due diligence obligation to terminate them. Even when lawful, however, we should always be mindful of the political costs of the exercise of extraterritorial enforcement powers on the territory of another state without its consent. Said otherwise, any "expansion of law enforcement hacking powers …. should balance law enforcement interests with competing foreign relations and national security".

DISINFORMATION. A POSSIBLE REGULATION OF LAW ENFORCEMENT INSTRUMENTS, BETWEEN EU AND ICT CONVENTIONS

Oreste Pollicino
Full Professor of Constitutional Law Bocconi University

There is no doubt that today more than ever courts are in a privileged position to identify risks of potential collision between interconnected legal regimes in terms of the protection of fundamental rights. Cooperation between courts forges closer ties between different yet interacting orders, while contributing to adapting legal systems to the new global challenges. The importance of this dynamic – and, more generally, the role and the impact of judicial activity – is even greater within the digital domain. Which are the reason of such "judicial amplification" in the cyberspace? There are at least two main reasons .

The main (substantive) reason focuses on the traditional gap between law and technology, where law lags behind technological advances. The burden of making up for this inevitable legislative inertia – at national and supranational level – falls heavily on the shoulders of the courts. The new factual and legal context created by the Internet has further extended this gap, thus highlighting the lack of judicial expertise to deal with the scenarios thrown up by new technologies. In this context, political inertia (which is not always forced as sometimes power is delegated to courts with a view to avoiding difficult choices) has fostered judicial imagination within the digital era.

The second reason is based on the judicial reaction to the cyberanarchy based approach.

The entrenchment of jurisdiction in internet cases was the best prove that Barlow, in his declaration of independence of cyberspace was wrong when he thought that public powers cannot regulate the cyberspace.

The approach of U.S. courts to the problems raised by the seemingly borderless nature of the Internet has moved from a reconsideration of the criteria they had set forth over time to determine the power of a court to settle disputes affecting, directly or indirectly, two or more legal orders.

With regard to certain matters, such as the exercise of freedom of speech, the U.S. case law has established the limits of personal jurisdiction in cross-border disputes on the grounds of the Due Process of Law clause of the Fourteenth Amendment.

It is worthwhile to look at these criteria in order to figure out how problems arising from the nature of the Internet have found solutions consistent with former rulings. In *Pennoyer v Neff*[56] the Supreme Court held:

The authority of every tribunal is necessarily restricted by the territorial limits of the State in which it is established. Any attempt to exercise authority beyond those limits would be deemed in every other forum […] an illegitimate assumption of power, and be resisted as mere abuse.

According to the *Pennoyer* Court, each State has jurisdiction "over persons and property within its territory".[57]

This decision reflected a concept of personal jurisdiction based exclusively on territorial borders, where the power of national courts to adjudicate lawsuits rests upon a contact between the forum state and the defendant or its property.

This approach turned out to be inappropriate as the growth of interstate commerce implied increases in litigation, and new technologies facilitated the circulation of people and goods. Thus, a harm could be inflicted and suffered in a certain state though neither the wrongdoer nor the injured party were physically present there.

Therefore, in *International Shoe Co. v Washington,*[58] the Supreme Court, even if not explicitly, overruled *Pennoyer* and worked out a more flexible test relying on the achievement of a minimum contact between the defendant and the forum state. In particular, the Court specified:[59]

But now that the *capias ad respondendum* has given way to personal service of summons or other form of notice, due process requires only that, in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend "traditional notions of fair play and substantial justice".

The minimum contact test did not provide a fixed rule, but required a specific and in-depth factual inquiry in every case when jurisdiction over the defendant was at issue.

Additionally, in *Hanson v Denckla,*[60] the Supreme Court further developed the minimum contact test, by requiring from the defendant an act that

56 Pennoyer v Neff [1878] 95 U.S. 714.
57 Ibid.
58 International Shoe v State of Washington [1945] 326 U.S. 310.
59 Ibid 326.
60 Hanson v Denckla [1958] 357 U.S. 235.

constituted a "purposeful availment" of the benefits and protections of the forum state.[61]

An important application of these criteria in the field of tort law is illustrated in *Calder v Jones,*[62] where the court developed the "effects test". The plaintiff had filed suit in California against two reporters, living and working in Florida, who had authored an allegedly defamatory article published in a newspaper that circulated in California. The Supreme Court found that California had jurisdiction, since, under the circumstances, petitioners must "reasonably anticipate being ha[u]led into court there' to answer for the truth of the statements made in their article". An individual injured in California need not to go to Florida to seek redress from persons who, though remaining in Florida, knowingly cause the injury in California.[63]

More in detail, the Supreme Court set forth a three-prong test, pointing to the awareness of the defendant about three circumstances: first, the allegedly defamatory article circulated in California; second, the plaintiff resided there; finally, the allegedly defamatory statements would have harmed the reputation of the plaintiff there.

How did such test affect the growing up of relationships by means of the Internet? Jurisdiction began to be felt as a key issue, since the development of the Internet implied that interactions seemed to take place anywhere and nowhere.[64]

What the American courts did when addressing the development of legal relationships on the Internet was attempt to adapt the outcomes of its endeavours to such a new, apparently borderless, environment. Some important "refinements" were needed.[65] In so doing, the judges distanced themselves from the approach of those who had sustained that the Internet could not be subject to legal regulation.

A further development of the criteria listed above was provided in 1997 in the landmark case of *Zippo Manufacturing Co. v Zippo Dot Com, Inc*.[66] In *Zippo*, the District Court for the Western District of Pennsylvania worked out the famous "sliding scale test", by distinguishing websites according to three levels of interactivity:

---

61 Ibid 253.

62 Calder v Jones [1984] 465 U.S. 783.

63 Ibid 790.

64 JL Goldsmith (1999).

65 U Kohl, Jurisdiction and the Internet. Regulatory Competence over Online Activity, (Cambridge, Cambridge University Press 2007).

66 Zippo Manufacturing Co. v Zippo Dot Com, Inc. [1997] 952 F. Supp. 1119 (W.D. Pa.).

The likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of the commercial activity that an entity conducts over the internet. At the outset, the court focused on subjects operating websites with the purpose of doing business:

If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper.

Secondly, the court pointed out that passive websites, unlike the former, are used only to post information and make it available in other countries, so that such kind of activity does not constitute a sound basis for personal jurisdiction. Last, the court held:[67]

The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the web site.

On such grounds, the District Court concluded that Zippo Dot Com, a Californian corporation, had entered into contact via its website with Pennsylvania residents with the purpose of doing business.

Not only American courts have faced problems of jurisdiction over the Internet. Another landmark case regarding a claim for online defamation was addressed in 2002 by the High Court of Australia. In *Dow Jones & Company, Inc. v Gutnick*[68] the plaintiff filed a complaint for defamation against the defendant, a financial information firm, due to an article that appeared in its online newspaper. Few of its subscribers were located in Australia, but the High Court adjudicated the case, holding:[69] "If people wish to do business in, or indeed travel to, or live in, or utilise the infrastructure of different countries, they can hardly expect to be absolved from compliance with the laws of those countries. The fact that publication might occur everywhere does not mean that it occurs nowhere"

It is well know how the issue of entrenchment of jurisdiction has been also crucial for the European Courts, as Google Spain case show, to asses European digital sovereignty (and European Values) over the tech companies with their server farm in United states

If the migration of constitutional ideas related to the entrenchment of jurisdiction has been a successful exercise, it cannot be the same as far as disinformation is concerned.

"The internet is a new free marketplace of ideas." This is the preferred

---

67 Ibidem

68 Dow Jones & Company, Inc. v Gutnick [2002] HCA 56.

69 Ibid 186.

metaphor of those who within scholarly and public debate take the view that the issue of fake news need not be addressed (and confronted) by public authorities (and public law). As underlined by Jacobs, the constitutional protection of free speech aims to facilitate representative democracy and promote individual autonomy. These values lead to the distinction between government regulations of speech, and speech regulations that are content-neutral.

Consequently, according to the marketplace of ideas paradigm, if it is true that under the First Amendment,t here is "no such thing as a false idea" in the material world,[70] this is even truer in the digital word, thanks to the enhanced opportunity to express thoughts. In other words, public authorities should not have any role in dealing with the ever-growing phenomena of disinformation on the internet, because users are (optimistically) supposed to have all the tools they need in order to select the most convincing ideas and true news, disregarding news that is not convincing or fake.

This position underlines an expression of complete trust in the capacity for self-correction of the market for information. However, the real challenge is how such a process of verification should be conducted according to the champions of the free market of ideas metaphor, since by definition scarcity of resources is an analogue and not a digital limit, with the result that there is no need to protect pluralism of information on the internet, legal rules (and especially public law) should take a step back in the name of the alleged self-corrective capacity of the information market. Just as the economic market knows no test of product "validity" but allows demand to drive supply, relying on the market to distinguish between viable and shoddy products, the best way of dealing with the phenomenon of disinformation in the information market is to secure the widest possible dissemination of all news, including news from contradictory and unreliable sources.

When the European Commission decided to import from the US constitutional humus the idea of free market place of ideas, there was a kind of rejection effect in the light of the different constitutional humus which characterises European Constitutionalism

The idea was to invest in the self-regulation of free market of ideas as far as the European fight of disinformation is concerned

In terms of policy making this idea was translated in 2018, into the adoption of a Code of Practice on Disinformation.[71] This was a soft law instrument under which platforms undertook – on an exclusively voluntary ba-

---

70 Gertz v. Welch, 418 U.S. 323 (1974).

71 EU Code of Conduct on Disinformation, https://ec.europa.eu/newsroom/dae/redirection/document/87534, 20 settembre 2018.

sis – to adhere to a series of commitments and standards in order to ensure better quality information. In addition, again in the same year, the Commission draw up an Action Plan against Disinformation in concert with the High Representative of the Union for Foreign Affairs and Security Policy.[72] It specified, amongst other things, that the coordinated Union response should be based on improving the capabilities of institutions to detect, analyse and expose disinformation; strengthening coordinated and joint responses to disinformation; mobilising the private sector to tackle disinformation; and supporting initiatives to raise awareness and improve societal resilience.

The strategy adopted during this second phase pursued a self-regulatory approach in this area, which was thus in some sense close to the US model and the metaphor, typical of that model, of the "free marketplace of ideas"; however, it soon proved to be unsatisfactory. Specifically, the substantial failure of the Code of Practice was cast into sharp relief, above all in the wake of the outbreak of the pandemic in 2020[73] and the Russian invasion of Ukraine in 2022. Moreover, almost in parallel with the adoption of these strategies, some nation states had chosen to pursue (or, as we shall see below in relation to Italy, attempted to pursue) much more far-reaching options.

The trailblazer in this area is without doubt the German Network Enforcement Act (*Netzwerkdurchsetzungsgesetz*, NetzDG),[74] the stated aim of

---

72 Joint Communication JOIN(2018)36 of 5 December 2018 from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the Action Plan against Disinformation.

73 In particular, European Commission, «Assessment of Practice on Disinformation – Achievements and areas for further improvement», SWD(2020)180, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69212, 10 settembre 2020, p. 19: «[*T*]*his overall assessment highlights that … the Code should be further improved in several areas by providing commonly-shared definitions, clearer procedures, more precise commitments as well as transparent key performance indicators and appropriate monitoring, all taking into account applicable regulatory frameworks. Further efforts should also be made to broaden the participation to other relevant stakeholders, in particular from the advertising sector*».

74 *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken.* On the law, see inter alia Victor Claussen (2018), Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation, Rivista di diritto dei media", 3, pp. 110-136; Thomas Wischmeyer, «*What Is Illegal Offline Is Also Illegal Online: The German Network Enforcement Act 2017*», in Bilyana Petkova e Tuomas Ojanen (a cura di), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries*, Cheltenham, Edward Elgar, 2020, pp. 28-56; Nannerel Fiano, «Il linguaggio dell'odio in Germania: Tra *Wehrhafte Demokratie* e *Netzwerkdurchsetzungsgesetz*», in Marilia D'Amico e Cecilia Siccardi (a cura di), La costituzione non odia: Conoscere, prevenire e contrastare l'hate speech online, Torino, Giappichelli, 2021, pp. 155-165; Mathias Hong (2022), «Regulating Hate Speech and Disinfomration Online While Protecting Freedom of Speech as an Equal and Positive Right – Comparing Germany, Europe and the United States», Journal of Media Law, 14, pp. 76-96.

which is to combat the spread of illegal content online, including numerous instances of hate speech and disinformation.[75] The NetzDG imposes a variety of obligations on operators of social networks and video-sharing platforms with the aim, first and foremost, of achieving greater transparency as regards their policies and practices on the moderation of unlawful content, and secondly of putting in place "notice-and-take-down" mechanisms. These involve, in practice, the adoption of procedures that enable users to notify providers concerning the presence of any unlawful content on the platforms operated by them. If a report is made, the provider is obliged to respond and, if the content does indeed violate any provision of the German Criminal Code, to remove it within a short period of time. Providers are liable to massive fines if they systematically fail to comply with these obligations.[76]

On the other hand, in 2018 France enacted various legislative measures in order to combat the "manipulation of information",[77] with a particular focus on its impact on elections. These initiatives were moreover launched in the wake of the fake news that blighted the 2017 presidential election campaign, even though it did not have any significant effect on the outcome. The specific legislation applicable during elections imposes first of all a number of additional transparency requirements, including an obligation to publish the source and amount of any payments received by platforms. Secondly, it provides for a special procedure before the courts as well as an administrative procedure before the *Authorité de régulation de la communication audiovisuelle et numérique* (ARCOM) aimed at stopping the spread of disinformation via public online communication services and also impeding the broadcast on

---

75 In reality, the law does not introduce a specific definition of disinformation (nor of hate speech), but merely refers to a series of offences already identified in the Federal Criminal Code. There is therefore no legislative recognition of an autonomous legal identity for the phenomenon of disinformation.

76 This law has been the subject of much criticism, not only from the managers of the platforms themselves, but also from activists and academics who have highlighted the risks of this legislation in terms of protecting freedom of expression. Indeed, the imposition of obligations to moderate illegal content could lead digital platforms to engage in forms of 'collateral censorship' that are potentially harmful to the rights of internet users themselves. See inter aliaHeidi Tworek e Paddy Leerssen, «An Analysis of Germany's NetzDG Law», www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf, 15 aprile 2019; Isabelle Canaan (2022), «NetzDG and the German Precedent for Authoritarian Creep and Authoritarian Learning», *Columbia Journal of European Law*, 28, pp. 101-133. About "censura collaterale", see among others Jack M. Balkin (1999), «Free Speech and Hostile Environments», *Columbia Law Review*, 99(8), pp. 2295-2320, p. 2298.

77 *Loi organique n. 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information* e *Loi n. 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*.

radio and television of "false information" originating from third countries.[78]

In view of the need to avoid the failures of past strategies (including in particular the 2018 Code of Practice) whilst also ensuring a harmonised, unitary approach at supranational level, a "third phase" in the fight against disinformation in Europe appears to have started recently. It has been characterised specifically by the adoption of more far-reaching and impactful legislation at EU level.

In addition, the first and most significant development within this context has concerned the Code of Practice on Disinformation and its relationship with the new Digital Services Act (DSA). Indeed, as has already been noted in chapter 2, after the Code was found to be ineffective in 2018, the Commission started to work along two parallel tracks: first of all thoroughly overhauling the Code,[79] and secondly transforming it from an instrument of self-regulation into an instrument of co-regulation.

As far as the second aspect is concerned, Articles 34 and 35 of the DSA impose an obligation on providers of very large online platforms and of very large online search engines to put in place mechanisms for the assessment and mitigation of systemic risks involving, amongst other things, "any actual or foreseeable negative effects on civic discourse and electoral processes". This clause clearly engages directly with the problem of disinformation. At the same time, Article 45 DSA provides for the possibility of drawing up codes of conduct, generally at the instigation of the Commission, providing amongst other things for the taking of specific risk mitigation measures, as well as a regular reporting framework on any measures taken and their outcomes.[80] As mentioned in chapter 2, whereas these codes enable the Union to put in place adequate common standards, and hence to achieve targets more effectively, they also ensures greater certainty for providers as regards the risk mitigation measures that need to be implemented.

---

78 The new French law has also been the subject of some preliminary questions of constitutionality: one of the most significant problems concerned, in particular, the identification of what can actually be considered 'false'. In this sense, the *Conseil Costitutionel*, through an interpretative judgement of rejection, affirmed that, as a condition for the constitutional validity of the law, it is necessary that the falsity of the information can be objectively demonstrated, as well as the need for *le action judiciaire en référée* not to involve mere opinions, parodies, partial inaccuracies or exaggerations; moreover, the misleading nature of the disinformation and its impact on electoral procedures must be clear. See Cons. Const., sentence no. 2018-773 DC of 20 December 2018, para. 21.

79 See, in this sense, Communication COM/2020/790, cit.; Communication COM/2021/262 of the Commission of 26 May 2021 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Commission's guidance on strengthening the code of practice on disinformation, 26 May 2021, COM(2021)262.

80 DSA, art. 45, para. 2.

This explains the pre-eminent role that the new 2022 code has played in that, having particular regard to the rules laid down by the DSA on codes of conduct, it was adopted specifically with the core aim of operating not only as an interpretative instrument but also as a common standard for combatting disinformation in accordance with Articles 34 and 35.[81] Therefore, it is clearly apparent from the Strengthened Code of Practice adopted in 2022 that the Union has shifted from a strictly self-regulatory strategy towards a co-regulatory strategy. Adherence to the commitments provided for under the Code (which are much broader than those contained in its predecessor from 2018) is now backed up by the new Digital Services Act and as such – whilst not being mandatory – is at least strongly advocated.

However, the novel aspects of the new phase of the European approach to disinformation are not limited solely to a move beyond the primacy of *self-regulation* towards a more top-down intervention.

The shift from a self-regulation to co-regulation which has been described with regard the new (hard law based) developments in the governance of information online

More precisely, in recent years, the fundamental question concerning online information and the impact that it has on internal democratic values and processes has led to the adoption of additional legislative measures aimed at promoting a digital ecosystem that is commensurate with the EU's "constitutional" requirements. A particularly important development came with the approval during the first few months of 2024, and thus shortly before elections to the European Parliament, of two regulations intended of better regulate the dissemination of online journalism and online political advertising respectively. These were specifically Regulation (EU) 2024/900 "on the transparency and targeting of political advertising"[82] and Regulation (EU) 2024/1083 on media freedom – the latter commonly referred to also as the European Media Freedom Act (EMFA). [83]

The ultimate aim of Regulation (EU) 2024/900 was to introduce uniform EU rules to govern the dissemination and distribution of political adver-

---

81 See, among others, Matteo Monti (2022), «Lo *strengthened Code of Practice on Disinformation*: un'altra pietra della nuova fortezza digitale europea?» *Rivista di diritto dei media*, 2, 2022, pp. 317-321.

82 Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.

83 Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 on a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Regulation). See in particular, Oreste Pollicino e Federica Paolucci (2024), «*Unveiling the Digital Side of Journalism: Exploring the European Media Freedom Act's Opportunities and Challenges*», La Revue des Juristes de Sciences Po, ١.

tising, also and above all in the light of the fragmentary nature of previously applicable national legislation.[84] The preamble to the new Regulation once again shows that it aspires to strike a balance among inherently constitutional and democratic values. It does so first and foremost by ensuring a high degree of transparency as regards the distribution of political advertising, whilst ensuring that "the provision of political advertising is in full respect of fundamental rights",[85] as well as requirements related to the promotion of the digital market, and above all the need to protect the interests of providers of political advertising services – in particular "micro, small and medium-sized undertakings, which often do not have the resources to absorb or pass on the high compliance costs connected to the preparation, placement, promotion, publication, delivery or dissemination of political advertising in more than one Member State".[86]

As its title in any case suggests, Regulation (EU) 2024/900 is focused specifically on "targeting techniques", which are defined as "techniques that are used either to address a political advertisement only to a specific person or group of persons or to exclude them, usually with tailored content, on the basis of the processing of personal data".[87] It is clear that this new legislation operates at the intersection between data governance and online information governance, amending the rules governing the recourse to user profiling techniques for the purpose of distributing content as well as the very structure of the online digital ecosystem. The Regulation stresses how the usage of these types of automated decision making systems is associated with a risk of significant collateral effects in terms of the protection of fundamental rights and individual self-determination, in particular where "special categories of data" within the meaning of Article 9(1) GDPR are involved:[88]

Such processing of personal data has specific and detrimental effects on individuals' fundamental rights and freedoms, such as to be treated fairly and equally, not to be manipulated, to receive objective information, to form their opinion, to make political decisions and exercise their voting rights. Furthermore, it negatively impacts the democratic process as it leads to fragmentation of the public debate about important societal issues, selective outreach

---

84 Regulation (EU) 2024/900, op. cit., recital 9

85 Ibidem, recital 5.

86 Ibidem, recital 10.

87 Ibidem, art. 3(11).

88 Article 9 of the GDPR states: «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

and, ultimately, the manipulation of the electorate. It also increases the risk of the spreading of information manipulation and foreign interference.[89]

It therefore comes as no surprise that the Regulation subjects the usage of these techniques to significant restrictions. It requires, amongst other things, that the only valid legal basis for data processing for targeting purposes is express consent by the data subject. Moreover, it expressly prohibits these techniques morphing into forms of profiling that use special categories of data pursuant to Article 9(1) GDPR.[90] Lawmakers were clearly concerned about the possibility of undue interference in the very "cognitive freedom"[91] of internet users, which could have significant ramifications not only for individual rights but also, in the aggregate, for democratic and political decision-making processes.

Also the second legislative instrument mentioned, the European Media Freedom Act, is fully consistent with the European strategy of promoting online debate rooted in pluralism, greater transparency and better quality information transmitted through digital infrastructures. The changes introduced by the Regulation, especially as regards the goal of combatting online disinformation, will be examined in greater detail in chapter 4. At this juncture, it seems fitting that automation and the use of automated decision-making systems plays a particularly important role also within the EMFA, in particular as regards the need to establish sufficient guarantees to protect users in the face of undue interference in their personal freedom when searching for information.

Accordingly, the EMFA has provided for the creation of a specific "right to customise the media offering", i.e. the right:

to easily change the configuration, including default settings, of any device or user interface controlling or managing access to and the use of media services providing programmes in order to customise the media offering in accordance with their interests or preferences in compliance with Union law.[92]

The legal framework established by the two new Regulations adopted in 2024 appears once again to confirm the aspiration to move the Union into a new legislative phase, which has been defined as "digital constitutionalism". This approach seeks to imbue the law with democratic and constitutional principles and values, including the right to obtain pluralist, high-quality

89 Regulation (EU) 2024/900, cit., recital 74.

90 Ibidem, art. 18(1).

91 See also Oreste Pollicino (2021), «Costituzionalismo, privacy e neurodiritti», Rivista di diritto dei media, 2, pp. 9-17.

92 EMFA, cit., art. 20(1).

information, the right to self-determination in decision making and the right to free elections within the ambit of a new algorithmic society. Indeed, here too efforts have been made to strike a correct balance between on the one hand the interest in the full development of new technologies – which moreover have the potential to act as extraordinary powerful instruments for advancing democratic debate – and on the other hand the need to contain the risks associated with the emergence of algorithms and private digital actors as new players on the global stage.

Another particularly significant aspect concerns the active promotion of the values of information pluralism as well as the attempt to guarantee an overall improvement in the quality of media communication. This objective is pursued specifically by the new Regulation (EU) 2024/1083 approved in April 2024 on media freedom (European Media Freedom Act, EMFA),[93] which has already been discussed in chapter 2.

As previously indicated in the report on the proposal,[94] the main aim of the new Regulation is to support the fundamental role played by independent media within civil society, insofar as the media contribute to shaping public opinion, providing citizens with a variety of options and reliable information. With this outcome in mind, the stated aim of the Regulation is to guarantee media pluralism and independence, as well as pluralist and independent journalism. For instance, Article 4 introduces important rights and guarantees, which can be exercised by media service providers against the Member States. Article 5 sets out some safeguards in order to protect the independence of public media service providers. On the other hand, Article 6 imposes a number of transparency obligations on media service providers in general (concerning above all the identity of owners and financing bodies), as well as specifically on media service that provide news and current affairs content (to take appropriate steps to guarantee the independence of individual editorial decisions).

Moreover, the EMFA recognises the importance of digital media within the contemporary world, as well as the impact that online platforms' business models have in terms of their contribution to increasing polarisation and on-

---

93 Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2014 on a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Regulation). See in particular, Oreste Pollicino e Federica Paolucci (2024), «Unveiling the Digital Side of Journalism: Exploring the European Media Freedom Act's Opportunities and Challenges», *La Revue des Juristes de Sciences Po*, 1.

94 Proposta di Regolamento del Parlamento europeo e del Consiglio che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE, COM/2022/457.

line disinformation. It is also mindful of the risk to media independence caused by third country financing and/or control.[95] As such, the EMFA lays down interesting rules to govern relations between media service providers and providers of VLOPs, which seek to supplement the DSA with specific reference to the journalism sector.

In particular, providers of very large online platforms must incorporate a function that enables media service providers: to identify themselves as such; to declare that they are editorially independent from Member States and third countries; to declare that they are subject to regulatory requirements for the exercise of editorial responsibility in one or more Member States or that they adhere to a co-regulatory or self-regulatory mechanism that is "widely recognised and accepted in the relevant media sector in one or more Member States"; and to "declare that they do not provide content generated by artificial intelligence systems without subjecting it to human review or editorial control".[96] Once this declaration has been made and the media service provider has been recognised as having "professional" status, it will be treated differently as regards moderating activity on the platform. This involves, for instance, the prior notification of any decision to suspend the provision of intermediation services.

On the other hand, the EMFA also provides for the option of launching "structured dialogue" among the parties involved, the European Board for Media Services and civil society. The objective of this dialogue is to ensure an exchange of experiences and to develop best practices in the application of that moderation mechanism and the promotion of media pluralism on online platforms. The need to society from harmful content is specifically mentioned, including "disinformation and foreign information manipulation and interference".[97]

---

95 So EMFA, considering 3-4: «Nello spazio dei media digitali i cittadini e le imprese accedono e consumano contenuti mediatici e servizi di media, che sono immediatamente accessibili sui loro dispositivi personali, in un contesto sempre più transfrontaliero … Il mercato interno dei servizi di media però non è sufficientemente integrato ed è soggetto a una serie di fallimenti del mercato sempre più numerosi a causa della digitalizzazione. In primo luogo, le piattaforme online globali fungono da punti di accesso ai contenuti mediatici, con determinati modelli commerciali che tengono a basarsi sulla disintermediazione dell'accesso ai servizi di media e ad amplificare la polarizzazione dei contenuti e la disinformazione … In terzo luogo, il buon funzionamento del mercato interno dei servizi di media è compromesso da fornitori, compresi quelli controllati da determinati paesi terzi, che si dedicano in modo sistematico ad attività di disinformazione, o manipolazione delle informazioni e ingerenze, e sfruttano le libertà del mercato interno a fini abusivi, ostacolando in tal modo il corretto funzionamento delle dinamiche di mercato».

96 EMFA, art. 17.

97 Ibidem, art. 19(1).

The resulting legislation thus essentially seems to incentivise forms of cooperation among online platforms, European authorities and media service providers. The specific underlying aim is to protect the spread of independent, pluralist and correct information, to combat fake or polluting content originating also (although not exclusively) from foreign countries and finally to enhance network users' self-determination in relation to information (and decision making).

Finally, a third aspect of particular significance concerns the acknowledgement at European level of the close interlinkage between disinformation and AI, as well as the impact that this interlinkage has on the proper operation of internal democratic processes. This acknowledgement reflects the renewed awareness (described above in chapter 2) of the paradigm shift that recent developments relating to artificial intelligence – and in particular progress in machine learning, generative AI, LLMs etc. – have brought about on the global technological and social scene.

In general, as it has been tried to show, it is clear that the EU's new approach seeks to engage on multiple fronts with the various aspects of disinformation. This involves, as the next chapter will show, a focus in particular on how disinformation interacts with the development and dissemination of AI on the one hand, and with the consequences for the media (and by extension, for democratic processes) on the other hand. Moreover, this multi-front approach appears to be characterised by a strong tendency on the part of the EU to move beyond the purely diplomatic, communicative strategy of phase one, and the self-regulatory approach of phase two, towards a co-regulatory form of disinformation governance, or indeed in some cases full-blown hard law.

IA SYSTEMS AND MODELS FOR STRENGTHENING NATIONAL CYBERSECURITY. PRESERVING EVIDENCE BY COUNTERING CYBER ATTACKS

Nunzia Ciardi
Deputy Director of the Italian National Cybersecurity Agency

Artificial intelligence and, in particular, generative intelligence, although a relatively recent manifestation of a technology that has existed for decades, is part of a heterogeneous and complex scenario, raising fundamental questions about the concepts of sovereignty, jurisdiction and territoriality. Its introduction has the potential to further destabilise existing paradigms, making the need for legal and political rethinking even more urgent. Indeed, these emerging technologies are profoundly changing the global regulatory and policy environment, challenging the effectiveness of traditional regulatory instruments and requiring an interdisciplinary approach to address their socio-economic and geopolitical implications.

Artificial intelligence is, therefore, a key element in shaping the future geopolitical balance, favouring those nations that will be able to govern it with efficiency and foresight. It is not surprising, therefore, that major global powers, such as the United States, China, Saudi Arabia, and several other nations, are investing significant resources in the development and application of AI. The scale of investment in this field is not only about building technological capabilities, but also about creating an integrated ecosystem that supports innovation and control of this strategic technology.

Artificial intelligence, in itself, is not a radically innovative technology: its potential lies in the extraordinary amount of data available today and the increasing computational capacity. The availability of these two factors is expanding at a dizzying pace, raising the question of who actually owns the data and, consequently, de facto control of the algorithms that are "trained" on them. These data often do not belong to individual states, organisations or companies, thus introducing important geopolitical, economic and social implications. The ability to collect and use these tools in fact determines a significant competitive advantage at the international level, increasing the gap between the countries that have the resources (data and computational power *in the first place*, but also talent) to exploit these technologies and those that, instead, not possessing them, are excluded.

AI is thus based on two "pillars": the availability of so-called "*big data*" and an advanced computational capacity, factors that, as we have said, are rapidly becoming central in the global landscape. Suffice it to say that, by 2024, the number of Internet users will have reached almost 5.5 billion, corresponding to about two thirds of the world's population. In addition, the number of connected devices has exceeded 8 billion, helping to generate a volume of data that is crucial for training AI models. The proliferation of connected devices and their increasing ability to interact with each other without human intervention are creating a highly complex digital ecosystem in which the quantity and quality of available data is set to grow exponentially.

Such a scenario poses significant challenges to national and international security. The ability of artificial intelligence to process huge amounts of data in a very short time makes it an extraordinary opportunity, but also a potential vector or "facilitator" of very serious threats. A striking example is that of the so-called *deep fakes*: the ability to generate false, but highly realistic video content has already demonstrated its dangerousness: in addition to the increasingly insidious and verisimilar scams, think of the potential political, economic or public security impacts that could arise from the dissemination of, for instance, false statements by a political or government figure, going so far as to jeopardise political stability and trust in institutions.

Even seemingly more ordinary threats, such as *phishing*, are becoming increasingly sophisticated through the malicious use of AI, becoming almost indistinguishable from legitimate, real communications. These attacks are not only capable of deceiving ordinary individuals, but also of targeting the most structured organisations, with potentially devastating consequences. Furthermore, advanced algorithms can be used to analyse codes in search of vulnerabilities in computer systems, automating the search for targets. *Malware* with "self-training" capabilities pose a further danger: once introduced into a system, they are able to continuously improve their evasion and infiltration strategies. These considerations become even more topical and relevant when one addresses critical or sensitive infrastructures, such as healthcare infrastructures: an attack against even a single local healthcare company - on which several facilities, hospitals and health centres depend - can in fact have considerable impacts, with cascading effects that go far beyond the individual affected.

A further aspect, which should not be overlooked, is that the AI itself, as an algorithm, is attackable. This can be done in various ways: by "poisoning", for instance, the very data on which it is trained. This phenomenon is extremely insidious, since it entails the risk (in itself already intrinsic to the

AI itself, since its internal decision-making processes are characterised by "opacity") of introducing unexpected, misleading or even dangerous results, thus irreparably compromising its reliability: if the data feeding the algorithms are altered, the applications based on them will also be altered, with significant consequences on the *outputs* produced by these technologies that, it must be remembered, are and will be increasingly present and pervasive.

In this context, the concept of resilience becomes crucial: like the mother of Winnicott, the well-known British psychoanalyst and paediatrician of the last century, perfect security "does not exist", there is "good enough" security. Even with highly sophisticated defences, there is always the possibility that a threat will go unnoticed or that a particularly elaborate attack will overcome the protective measures. The important thing, and this is where resilience comes in, is to develop the ability to get back up, recover and react after the blow suffered, restoring systems to operability and ensuring continuity of services as quickly as possible, minimising the negative consequences.

Consider, again, the example of the health sector: a successful attack, in such cases, could lead to the interruption of essential services and life-saving therapies, blocking emergency rooms, ambulances and operating theatres. And it is a phenomenon that affects not only Italy, but all the most advanced countries. For this reason, it is essential to implement measures that minimise the damage caused by an attack and ensure the fastest possible restoration of services.

With this in mind, the National Cybersecurity Agency (NCA) has adopted the concept of resilience as a guiding principle, with the aim of ensuring the timely recovery of compromised systems and thus also protecting national security in cyberspace. This translates, concretely, into operational practices ranging from the design of more robust systems to the training of specialised personnel, and the creation of coordinated response protocols involving both the public and private sectors.

Cyber resilience has recently received an important legal recognition through Law No. 90/2024, which, in addition to regulating more extensively the operational relations and information links between ACN, Judicial Authorities and Judicial Police, has introduced appropriate balancing mechanisms between investigative and national resilience needs, functional to ensure the effective and timely conduct of recovery activities, the assurance of evidence sources and the coordination of the National Anti-Mafia and Anti-Terrorism Prosecutor (PNAA).

In particular, the law stipulated that the Agency must inform the NAPA when it learns of an attack against certain computer or telematic systems and, in any case, when a subject is affectedof the National Security Perimeter, NIS

or Telco , and that the Public Prosecutor (PM) informs the NAPA when he learns of certain serious computer crimes, also ensuring the information link with the CNAIPIC. In addition, the same law introduced specific balancing mechanisms between investigations and resilience, providing: on the one hand, that the PM shall issue the necessary provisions to ensure that urgent investigations are carried out taking into account the activities carried out by the Agency for resilience purposes; on the other hand, that, in order to avoid a serious prejudice for the course of the investigations, the PM may order the deferment of resilience activities with a reasoned order.

An emblematic case was the arrest of a young *hacker*, who was responsible for an attack on the systems of the Italian justice system: thanks to the cooperation between ACN, DNA, the investigating Public Prosecutor's Offices and the Postal Police, it was possible to secure the compromised systems without affecting the ongoing investigations, thus ensuring the continuity of critical services while respecting the investigative needs. This experience demonstrated the effectiveness of a coordinated and synergic approach to the management of security incidents - which are also crimes, but not limited to -, highlighting the importance of cooperation between the different institutions involved.

The cyber domain is a domain unlike any other: it is transversal, multifaceted and changeable. It is a domain in which we are all personally immersed. Consequently, it must be recognised that cyber resilience and security rest on the shoulders of each and every one of us: on every single company, on every single institution, on every single citizen. Only through a holistic approach, therefore, will it be possible, if not to eliminate it, then to reduce cyber risk to at least a "physiological" level.

For such an approach to be fully realised, it relies on a fundamental element: culture. We can spend millions on securing systems, but if an employee does not take all the necessary precautions and, for example, while *smart working*, connects the service computer to the home network without precautions, any investment risks proving futile Due to a lack of security culture, the overall effort of an entire organisation is thus thwarted. It is therefore crucial to invest in training and spreading awareness of cyber risks at all levels and in all sectors, especially with regard to the challenges and opportunities offered by new technologies in an increasingly digitised world.

In conclusion, returning to the topic of artificial intelligence, which is emblematic of the era we are living in, I would like to close by reiterating that AI offers extraordinary opportunities, but also poses enormous challenges, particularly with regard to national security in cyberspace, and beyond. In such a scenario, characterised by the spread of AI as a potential offensive,

defensive and attack platform, resilience will prove to be an even more crucial element in ensuring the stability and security of our country in the face of new, emerging or simply different threats.

The future of national security, but also that of our own security, will depend on our awareness and ability to integrate advanced technologies, develop effective defence and resilience strategies, and ensure that responses to attacks are coordinated and proportionate to threats. Ultimately, resilience, enabled by culture, is not only a defensive strategy, but also a key component of a country's ability to thrive in an increasingly digitised and interconnected environment.

THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE: A NEW MODEL OF INDEPENDENT SUPRANATIONAL PROSECUTOR ENSURING EFFECTIVENESS AND LEGAL COMPLIANCE

Danilo Ceccarelli
EPPO - Senior Coordinator, Fight against Organised Crime

Introduction on the EPPO

The EPPO "is established as a body of the Union" (Art. 3 of the EPPO Regulation)[98], more specifically as the Prosecutor's Office of the Union. It is tasked with "investigating, prosecuting and bringing to judgment" the perpetrators of criminal offences affecting the Union's financial interests (Art. 4) and acts "in the interest of the Union as a whole" (Art. 6). Within the EU institutional architecture, the role of the EPPO is very peculiar, and unprecedented. The EPPO does not rely on national prosecutorial authorities. The EPPO investigates and prosecutes in the Member States directly, without national intermediaries, exercising prosecutorial and investigating powers. In line with Article 86 TFEU, the EPPO exercises its functions before the courts of the Member States.

This is especially reflected in the provisions (Arts. 4, 13(1), and 28 to 40), that confer on the European Delegated Prosecutors (EDPs), who are based in the Member States, as a minimum, the same powers as the national prosecutors. This creates a hybrid structure, where the EPPO is the centralised prosecutor's office of the Union but has also full prosecutorial authority within the national system of each Member State.

The EPPO as a fully independent prosecution service

A specific, and probably the most important feature of the EPPO, is its external independence. There are different models of prosecution in the EU Member States. In some Member States, the prosecution service has strong ties with the executive power and may be subordinate to instructions from the government or it is required to report to it. In other few Member States, in order to balance the lack of the independence of the prosecutor, there is an (obviously independent) investigative judge with strong investigative pow-

98 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('EPPO'), OJ L 283, 31.10.2017, 1. In this document, the legal provisions quoted are taken from the EPPO Regulation, unless otherwise indicated.

ers. In other Member States, however, the prosecution service is independent, and the prosecutors are fully part of the judiciary.

The EPPO Regulation emphasises the independence of the EPPO in its Art. 6 and recital 16, prohibiting any kind of interference and influence from any authority of the Union and of the Member States and from any persons external to the EPPO. According to Arts. 6(2) and 7, the EPPO is accountable to the EU and the Member States for its general activities but not for its specific investigations and cases, which are protected by confidentiality and only subject to judicial control in line with Art. 42 of the Regulation and national law.

Furthermore, the EPPO does not have links with the executive power even as regards its general prosecutorial policy. According to Art. 9 of the EPPO Regulation, the College of the EPPO takes decisions on strategic matters and is tasked with ensuring coherence, efficiency, and consistency in the prosecution policy of the EPPO throughout the Member States. Granting the EPPO the authority to elaborate and decide internally its prosecutorial strategy and policy, without either being subject to general instructions from the executive power, or to directives, guidelines and instructions from a hierarchically superior prosecutorial authority linked to the government, means granting to the EPPO full external and internal independence. This is further confirmation of EPPO's independence and a clear severance from the executive power.

Finally, recital 16 of the Regulation clarifies the link between the investigative and prosecutorial powers conferred on the EPPO and the necessity to safeguard its independence: "since the EPPO is to be granted powers of investigation and prosecution, institutional safeguards should be put in place to ensure its independence." Therefore, the current statutory rules and institutional framework guarantee that the EPPO, acting as a single office in all the participating Member States, is not exposed to risks of being subject to instructions from or being obligated to report to the executive in specific cases.

However, safeguarding the independence of the institution might not be sufficient to protect the independence of the prosecutorial functions as a whole. As any other prosecution service, the EPPO carries out its mandate through its prosecutors, namely the European Chief Prosecutor (ECP) and the European Prosecutors (EP), acting as members of the Permanent Chambers, as well as the European Delegated Prosecutors (EDP). Hence, institutional safeguards should be in place to protect the EPPO as single office but also to protect its prosecutors' statutory independence and their institutional status. Institutional safeguards to ensure the independence of prosecutors include their appointment, career progression irremovability, dismissal, and disciplinary action.

As regards the appointment procedure, the EPPO cannot be considered fully independent as far as the appointing authorities of the European Chief

Prosecutor and of the European Prosecutor are EU political institutions. Moreover, the appointment procedure of the European Prosecutors is characterized by a notable lack of transparency. Depending on the Member State involved, also national political authorities could have a role in the appointment procedure – including that of the European Delegated Prosecutors, where in any case the final decision making is in the hands of the College of the EPPO.

Furthermore, political authorities can hamper judicial independence also by means of other, more subtle, methods, such as cutting the operational budget or not allocating enough resources to the prosecution service, thus consistently reducing its efficiency and effectiveness.

The legality principle and the duty of investigating and prosecuting exclusively in compliance with the applicable Law

In any case, once they are appointed, the European prosecutors of the EPPO enjoy the necessary institutional safeguards to protect their independence. This is even more notable if we consider that the prosecutorial activity of the EPPO – differently from a few of its participating Member States – is governed by the legality principle, as emphasised in recitals 66 and 81 of its Regulation. This means that the EPPO does not have the discretion not to investigate and prosecute an offence for which it exercised its competence, as it is also clear from the wording of Articles 25(1), 35 and 36 of the Regulation.

As in any democratic system where the prosecution service enjoys full independence, the executive power lays out its political decisions by means of legislation. The EPPO is subject, first and foremost, to EU Law, starting from the Charter of Fundamental Rights, and, in line with the principle of primacy of EU Law, to the national legislation where applicable, provided that this is not in contrast or incompatible with EU Law.

As a consequence, the action of the EPPO is strictly bound only by the applicable Law.

This ensures that the investigative and prosecutorial policy of the EPPO is legally predictable and is in line with the protection of the values that are enshrined mainly in the EU Charter of Fundamental Rights and in the Constitutions of the Member States of the EU. Similarly to the Court of Justice of the Union, the EPPO defends the constitutional values of the European Union, which are shared by the Member States and define the very identity of the European Union as a common legal order.[99] In this context, the EPPO is protected by political interference in its investigations, be it from authorities of

99 CJUE (Grand Chamber), 16 February 2022, case C-156/21 (Hungary v European Parliament and Council of the European Union), paragraph 127.

the Member States or of the Union that – depending on the political context - could have a very peculiar reading of the kind of "public interest" they want to protect. In a supranational and complex environment such as that the EPPO operates in, this protection is even more necessary in order to have an investigative and prosecutorial action guided only by law, and not by possible instructions of political authorities.

This necessity is even more obvious when referred to criminal phenomena such as cyber criminality, which could threaten infrastructures or democratic institutions, and could endanger fundamental values of the Union and of its Member States. In these situations, the law should be the exclusive binding element on the prosecutorial authority in charge of implementing and confirming countermeasures and responses to the threat. Only this way, effective protection is ensured.

Independence, supranationality and effectiveness of the EPPO

In a context of cross-border, but also of border-free criminality, the EPPO can be presented as a model also in terms of efficiency and effectiveness of its action.

The most apparent feature of the EPPO is its supranational dimension, being the first ever prosecution service with direct investigative and prosecutorial powers in 24 participating Member States.[100] In this context, the EPPO has a very specific knowledge of cross-border jurisdiction issues, and a unique experience of the operational and legal systems of the EU member States, which the EPPO experiences on the field and in national courtrooms every day.

The EPPO is a single office, a dimension that includes both its central and its decentralised structure and, as such, it does not suffer from the fragmentation that, in several Member States, affects the prosecution service, often organised in many separated – and sometimes competing. Prosecutor's offices. The EPPO carries out its cross-border investigations not based on the principle of cooperation, or as a network of prosecutors, but as a prosecutor's office where the operational activity is coordinated internally. In this way, the office is able to achieve a consistency that is very different from what is being experienced in the traditional cross-border cooperation in criminal matters.

---

100 The participation of Member States in the EPPO is based on the principle of enhanced cooperation, in line with Articles 326 to 334 of the Treaty on the Functioning of the European Union, which allows some Member States to agree to pursue an objective among themselves even if the other Member States choose to abstain from participation. On 1 June 2021, when the EPPO took over its investigative and prosecutorial tasks, 22 Member States were members of the EPPO. Poland joined the EPPO on 29 February 2024, while Sweden became a member on 16 July 2024. Hungary, Ireland and Denmark are not members of the EPPO.

However, the EPPO works, at the same time, in a system where Law Enforcement is the national authority. Thus, the EPPO needs to integrate the activity of Law Enforcement in its supranational structure. This is happening out of the traditional tools (EU and international) on mutual cooperation, such as the EIO or the JIT, but conferring on the EPPO the authority to instruct and direct the national authority while conducting the investigation, in line with Article 28 of the Regulation, in all its Member States. This way, national Law Enforcement that work under the direction of the EPPO became somehow "supranational" in the framework of the concerned investigations.

Therefore, efficiency and effectiveness in EPPO's cross-border investigations are – to a large extent– a consequence of the supranational nature and of the structure of the EPPO. Of course, in order to make this possible in practice, it is necessary that the EPPO has at its disposal enough investigative and analytical tools and specialised and skilled personnel that work alongside national Law Enforcement, within the logic of the "single office". So far, this is being ensured thanks to the Operations Unit of the EPPO, but a very important role is also played by EUROPOL that, although not having the authority of "judicial police" or "law enforcement", is the EU Agency that is best placed to work hand-in-hand with the EPPO and the national authorities, and has exceptional analytical support capability. There is no doubt, in fact, that supranational organisations with investigative, operational, prosecutorial and – if necessary – judicial authority can reach a degree of effectiveness in pursuing serious cross-border criminality that is otherwise impossible following the traditional path of inter – governmental cooperation.

This is even truer when fighting cyber criminality and cyber threat, where borders and jurisdiction are shifty and uncertain. Undoubtedly, criminal phenomena where the concept of territorial jurisdiction is dematerialised are growing, and this presents a challenge to the traditional rules on jurisdiction that legal systems traditionally adopt, but especially to the investigative and operational capability of the interested countries. Rules on jurisdiction in this field use more and more often concepts such as the "protective principle", which takes into account the impact of cybercrime on the interests and security of the state, or anyway the possible adverse effect caused in the concerned country. Article 22 of the Draft United Nations convention against cybercrime[101] foresees that State Parties have the option to establish their jurisdiction based on the principle of passive personality. i.e. if the offence harms the State or their nationals. From the legal point of view, these rules could create

101 "Draft United Nations Convention against Cybercrime - Strengthening international cooperation in combating certain crimes committed through information and communication technology systems and for the sharing of evidence in electronic form of serious crimes", 7 August 2024.

conflicts between concurring jurisdictions, but they are not otherwise particularly problematic.[102]

Conversely, the disconnection between the territories from where the offence is initiated, and the territories affected by the conduct, creates enormous investigative and operational difficulties that is extremely hard to overcome via the traditional inter-governmental tools on mutual cooperation, both at police and at judicial level.

In this context, the EPPO could serve as an excellent example of a genuine supranational authority without significant jurisdiction constraint in its "legal area", and with a large supranational investigative and operational capability in its Member States, where it take action swiftly and effectively.

Conclusions

The EPPO exemplifies a unique model of an independent prosecutor's office, which takes action based on the legality principle and exclusively in compliance with the applicable Law, especially following the principle of primacy of EU Law. This supranational legal framework goes alongside supranational investigative capability and prosecutorial powers, thus displaying a remarkable operational effectiveness and ensuring the protection of fundamental democratic values.

102 In these situations, Article 22, paragraph 6, of the United Nations draft convention only provides 'if appropriate' that the interested parties 'consult one another with the aim of co-ordinating their actions'.

THE PROTECTION OF FUNDAMENTAL RIGHTS IN VIRTUAL SPACE AND THE USE OF ADVANCED AI TOOLS, FOR EXAMPLE FOR SOCIAL CONTROL OR DISINFORMATION.

Amandeep Singh Gill
United Nations Secretary-General's Envoy on Technology

Good morning, from New York.

I am really pleased to be able to share some remarks with you and I would like to thank the foundation and the Italian G7 Presidency for this honour. The topic you have chosen for today is certainly very important, at a time when technology is making great progress in a sometimes unpredictable manner. Artificial intelligence, in particular, is one of these powerful technologies that is reshaping our economies and will soon reshape our societies and also our political systems, basically. It is a technology that somehow behaves in the same way as human beings, in the same ways that humans communicate with each other. With the advent of broad language models we see how we act, how humans act, so does technology. There are, of course, worrying implications, but at the same time exciting opportunities to be able to make progress with regard to sustainable development goals and increased productivity in economies, but also in the context of an ageing population.

At the UN level, we are trying to figure out what is the space for international governance of these technologies. In fact, many governance actions and regulatory aspects will still be handled by national governments that will also take into account national security issues, specific cultural situations, factors relating to specific societies, and at the same time economic competitiveness factors. However, there are actions that somehow belong in the international context. These actions must offer value to both governments and the private sector. Therefore, at the UN level, we know perfectly well that we have to build on the values of the UN Charter, the Universal Declaration of Human Rights, and human rights treaties. Basically, we have to build on core values related to human rights, fundamental freedoms, the protection of democracy and the rule of law.

At the same time, given the location of the United Nations, we also have to think about what are the implications of these technologies for international collaboration. That is, there are ways to expand international collaboration using this technology, to somehow lessen the competition that will still exist, but we can manage the competition in a way that creates a space for

collaboration. So we have been very active in the last couple of years in this regard, and we have recently had some success in our summits with the adoption of a global pact, which is the first universally accepted agreement for the governance of artificial intelligence. This of course builds on the progress made during the Hiroshima process, which was then taken forward by the Italian G7 presidency, and what has been done at the Council of Europe and UNESCO level.

So what are the main elements of this universal agreement on artificial intelligence that was made last September? We need, first of all, to take a close look at the capabilities of artificial intelligence, so we need a constant evaluation of these capabilities so that we can assess the situation independently, beyond what companies or individual countries say. What is the significance of this technology in terms of opportunities? And this is somewhat similar to the climate change situation, where we have an intergovernmental group dealing with climate change. But this technology is moving fast. So we have to act fast and at a public level, to give politicians references on which to base their decisions. In addition to this international group of scientists, we have the leaders at the summit who have decided that constant political dialogue will be necessary. This is at the heart of the problem that is being discussed at the current conference, namely how to ensure a certain interoperability between jurisdictions, how to ensure that issues of crime, protection of individual liberties and fundamental rights do not clash. That's why we have different jurisdictions and, as we know, the United Nations is an inclusive platform that allows different jurisdictions, whether it's the United States, China, the European Union, to talk to each other and share a number of factors in order to learn from this exchange. At the same time, efforts are being made to build a common vocabulary to address issues using the backbone of the UN Charter and other valuable legal instruments.

A third aspect of the decisions taken is to build capacity globally, because today the public sector, especially police agencies, are a bit behind in understanding technology, as knowledge resides mainly in the private sector. It is important to be able to follow these technologies, act wisely, and also think about equity, because there is a digital divide. For instance, among the top 50 countries in terms of artificial intelligence capabilities, there are no African countries; the top African country is only 2000th in the list of artificial intelligence capabilities. This is why it is crucial to give access also to less wealthy countries, while preserving cultural and linguistic difference. To date, most data is only in one language and refers to a specific geographical area, which has implications for the future. These are three areas where decisions have been taken, but we still have a lot to do. Of course, the UN Secre-

tary-General has absolutely decided to continue this kind of work, supporting both the public and the private sector, which also has very important responsibilities, as emphasised in the outcome of the Hiroshima meetings.

Artificial intelligence is not just a topic for experts, it is something that affects everyone, because it will reshape our societies, the way we access information, the intermediation in many senses, and also the impacts on our relationships between people. We all have a mental capacity and will that is beyond the capabilities of any chatbot. This of course has meaning, and implies discussions about society. It implies that our regulatory systems, our jurisdictional mechanisms, were created to work in a different world. This implies that we all have to think about these issues and act. That is why I am really glad that you are paying attention to these issues. We are working closely with the Italian G7 presidency on the impacts of artificial intelligence. There are also many groups at the international level, such as the Vienna Group, dealing with crime, cybercrime, artificial intelligence and impacts such as disinformation, and how cybersecurity threats should be addressed in the future. I wish you all the best in your work and thank you once again. I would also like to remember the person after whom this foundation that organised the event was named.

DEBATE

Luigi Salvato:

I would like to thank my colleague Danilo Ceccarelli who has with such passion and thoroughness verified the possibility of crossing, of going down the road of apps to strengthen Cyber Crime jurisdiction. To summarise his report in a somewhat naive and somewhat provocative question: but then do we think of extending the jurisdiction of EPPO to Cybercrime as well? Anyway, leaving that question aside, we have concluded. Is there anyone? Are there any other questions?

Eric Do Val Lacerda Sogocio:

Thank you for the presentations. I have a fairly simple question for two of the speakers.

To Prof. Roscini: I heard your presentation, you talked about countermeasures and due diligence, but my small question is: wouldn't you be concerned about a situation where prosecutors could commit offences in jurisdiction? Could they commit the offence of illegal access or misuse of a device, misuse of a device, in pursuit of countermeasures, as you explained? But I would ask the same question to Dr Ceccarelli: how would he not be concerned about committing an offence, in another jurisdiction, in the investigation?

Marco Roscini:

It is not a simple question. I would be worried but I think we have to choose between doing something that might be illegal under criminal international law, and doing nothing. That is the choice. You cannot go down a dead-end street because there is the element of conduct, perhaps lawful, that is done under the shield of sovereignty. But in the end, if it is possible, there is that choice to be made, but the different interests must be balanced: the interest of the state whose territory has been violated and the right of the other state. In short, there are certainly cases where one has tried to balance the different interests. I referred to that Norwegian case.

The word "sovereignty" is perhaps the one most repeated at this conference, repeated over these two days, and is often used as a good value in itself. But international law does not protect sovereignty for its own sake, it protects that which respects the law. When one sovereignty violates the other sovereignty, so many protections disappear and so we come to countermeasures.

This is the principle of non-intervention, which protects a only state when it acts, even internally, according to the rules. So my answer is not an answer: I can only say that we have to balance the different interests. The state wants its sovereignty to be protected, but there is precisely this gap between prescriptive and enforcement jurisdiction that I mentioned earlier.

Danilo Ceccarelli:

I agree with Professor Roscini's answer and I also agree with most of what he said in his presentation. But I want to tell you something: prosecutors and law enforcement agencies commit crimes every day. We intercept people, we arrest people by depriving them of their freedom, we freeze and seize assets, and we do it every day. We put people in prison, sometimes for a long time, which is perhaps more the case with judges. But this can be an offence in itself, that is, the state defends itself, defends its community against illegal activities. The big difference is that this is done according to the law, and every time we take a step we accept a risk. Yes, it may be true that we do not respect the law and commit a crime by breaking it. Perhaps we do not respect, and this is something Professor Roscini mentioned, the principle of proportionality.

We think about what is happening in the world today. But we have to react according to the law, in good faith, as best we can against lawlessness, because if we don't, society... eh, I don't know how it would function without lawfulness.

So it is a risk we accept, it is part of our job, and this includes situations where we have to take an initiative and act against someone who is in a third country or even against a third country, always respecting the law and the principle of proportionality.

CONCLUSIONS

Alfredo Mantovano
State Secretary to the Presidency of the Council of Ministers

I apologise for not being among you as I would have wished, I greet you all and I thank the Occorsio Foundation for the invitation and a very special greeting to President Giovanni Salvi. With this seminar you have done an important thing, you have called for an in-depth reflection on the need for guarantees of jurisdiction in the resilience and defence of the national security of virtual space. The progressive development of digital technologies, from artificial intelligence to crypto-currencies, places, as we know, states and, within them, jurisdictions, in front of challenges and innovative threats that exploit spaces with completely unprecedented characteristics in the traditional sense; the category of extra-territoriality, related to physical spaces over which states do not have jurisdiction, except for some interpretative fantasy, which does not interest us at the moment. Speaking of Cyber instead, extra territoriality refers to spaces that are devoid of any geographical connotation and that are technically unlimited in size. It would be better to say that they are a-territorial phenomena as suggested by some authors, to highlight that their structural characteristic is precisely the lack of a physical territory. Appropriately enough, the seminar identified within this framework a series of new and complex problems on which to reflect, such as identifying an effective territorial connection criterion that roots the jurisdiction of states in relation to what happens in virtual reality. This applies first and foremost in terms of crime repression, but not only: I thinking of amprofiles of economic relevance, e.g. what impact artificial intelligence has on fundamental rights and the organisation of public functions, including jurisdiction. For instance, how the resilience of critical digital infrastructures can be effectively protected, and what are the problems associated with identifying the real direction of cyberattacks, i.e. the complex issue, both from a point of view technical-informatics and a political or diplomatic , of so-called *attribution;* how, finally, to coordinate at international level strategies to combat transnational crime in the digital world.

The government is not backing down, for its part, in providing an effective response to these challenges. I I I am also thinking of the adoption of the legislative decree of recall, among other things, the innovations made by Law No. 90 of 28 June this year to ensure the strengthening of national cybersecu-

rity, which am sure have all read you discussed, studied in depth and ; 4 September 2024 transposing the directive NIS2 and the bill on AI, currently under discussion in the Senate, which aims to combine the potential of AI with respect for fundamental rights and identifies guidelines for its use in public functions, including the judiciary.

International cooperation plays a fundamental role, and for this reason, in addition to the efforts made at the European level, we are seizing the opportunity of the G7 Presidency: as the Italian Presidency, we have set up a new working group specifically dedicated to cybersecurity, within which we will discuss with our partners the refinement of tools to combat the main cyber phenomena that threaten our security, *first and foremost ransomware* attacks. There is still much to be done, and in this sense initiatives like the one you organised are certainly useful and valuable, and I thank you.

I renew my greetings to you all.

SUMMARY OF WORKS

Giovanni Salvi

In reality, not only will I not draw any conclusions, but I won't even summarise the work, because it would take another half day to do so, given the complexity of the issues that were addressed. I will just say, by way of a conclusive summary, that the work group that developed this programme perhaps did not make a mistake in structuring the progression, because in the end we arrived, on the last day, at the crux of our theme, as is also made evident by the amusing exchange of words between Sogocio and our speakers today. It's funny because it gets to the heart of the matter, a point that cannot be overcome, at least for me, at the moment. I don't see a solution. The proposal that emerged in our preparatory work, and which I see today has found confirmation, is that a clear distinction must be made, also with regard to the activities of the jurisdiction in a virtual space in cyberspace, between what is ordinary judicial activity, for which current cooperation tools can be used, including the most modern ones we are imagining, those provided for by the European Union regulation on virtual evidence (e-evidence) and those provided for by the Budapest Convention and the future convention on cybercrime.

These are effective forms of cooperation and will become increasingly effective. But there is one point that cannot be addressed in this way, precisely because of the specific characteristics of this sector, because there are criminal activities, or in any case activities that require investigation, that cannot be investigated later, not even in the short space of hours necessary to request cooperation from another judicial authority. This, in my opinion, is a starting point.

Only by following the trail immediately, and this will not always be enough, will it be possible to collect and consolidate some evidence, which is sometimes essential. The same problem arises for criminal jurisdiction and for public international law in terms of attribution. It is exactly the same problem. Obviously the quality of the evidence is different, as is the reasoning that leads to the conclusion. But the problem is the same.

Here that question remains. It remains because, within certain limits, the proposal that emerged from many interventions is to use what is provided for both by the Budapest Convention and by the future convention on cybercrime: the transition from Investigative Teams to Investigative Bodies, that is

stable structures that are independent of the commission of the crime and stabilise consensus before the crime is committed.

These allow immediate action even by the attacked state, except for validation mechanisms, at any time the attack takes place and wherever the attack comes from. This is difficult, but it is a viable path. It is not the path of the European Public Prosecutor's Office, because that is the path of exercising jurisdiction from start to finish over attributed crimes.

I believe it is too early to predict, but we can use the experience of the European Public Prosecutor's Office and, above all, the mechanisms used to ensure the independence of a body dependent on the Union, to imagine the building of trust between the states that intend to participate in this form of sharing of structures.

There are already police structures that can be better organised around these objectives. But once this is done, and we have one hundred nation states participating in the Investigative Bodies that allow the transfer of a small part of sovereignty, not the jurisdictional sovereignty over the entire procedure, but the sovereignty necessary to immediately acquire information that would otherwise be lost. But there are still ninety other states.

The question that you have discussed so effectively, especially by Sogocio, Professor Roscini and in Ceccarelli's response, remains. It remains especially in relation to the most dangerous states and the most dangerous attacks.

Our objective is to work on this. For the Occorsio Foundation, today's work has two functions: to bring the acquired knowledge into daily practice and to combine it with training for magistrates and police forces. We thank all the speakers and especially the young people who collaborated, showing the best of Italy, despite the difficulties and sacrifices.

Finally, a fond thought for Eugenio Occorsio, who is currently facing a personal battle. His character, and that of his father, remind us of the importance of our commitment to legality.

***

Michele Giacomelli

Thank you very much. Actually, just two words to say that it has been a pleasure to have you here at the Farnesina. It has been very instructive, very interesting and it is a source of pride for us to have helped the Vittorio Occorsio Foundation to organise this initiative, to collaborate with you and to contribute to the scientific and human enrichment of our work. Thank you all very much.