The Diplomacy of Systemic Governance in Cyberspace

Alexandru GEORGESCU, **Adrian Victor VEVERA**, **Carmen Elena CÎRNU**
National Institute for Research and Development in Informatics - ICI Bucharest
alexandru.georgescu@ici.ro, victor.vevera@ici.ro, carmen.cirnu@ici.ro

Abstract: Cyber has become a cross-cutting issue affecting not just multiple domains, but all domains, both inside and outside the borders of any individual country and the jurisdiction of its legitimate and competent authorities. For this reason, cooperation becomes key in several aspects related to coordination of infrastructure build-up and use, general governance issues like retail crime and privacy, but also security issues, such as the protection of critical infrastructures, the protection against disruptive crime and the governance of inter-state conflict and terrorism issues. Outside of the realm of traditional diplomatic cooperation, we also find and define a systemic governance diplomacy, which is done by experts at the level of institutions and collectives in order to develop and promote standards which become part of the critical information infrastructure landscape. Of course, this is an area that also becomes the theater for inter-state competition.

Keywords: Critical infrastructure, Standards, Cyber diplomacy, Competition

INTRODUCTION

The twin phenomena of rapid technological advancement and globalization have engendered a significant dependence on the part of all states on information infrastructures, socio-technical systems, both physical, virtual and organizational which provide the data gathering, processing, transmission and communications required to coordinate interdependent critical infrastructures which are distributed geographically. The system is more widely distributed and more complex than any one country, no matter how powerful, can successfully govern. Diplomacy must come into play in order to provide the necessary political capital, institutional constructions and coordination capacity that allows interdependent nations to protect their critical infrastructures, including and especially their critical information infrastructures. Criticality, in every such case, is in the eye of the beholder, but generally refers to the scope and severity of the disruption, human losses and material damage, not to mention prestige and confidence losses, which the disruption or destruction of said infrastructure would engender (Georgescu et al, 2019). These infrastructures face a complex and challenging security environment, dealing not just with deliberate threats of a hybrid nature from myriad actors, but also the emerging risks, vulnerabilities and threats which complex and interdependent distributed systems tend to produce, alongside unpredictable cascading disruptions (Katina et al, 2014).

Therefore, we have steadily seen the rise of a new field of diplomacy, cyber diplomacy, and a new subfield, the diplomacy of systemic governance in cyber (but also other sectors). In this field, it is not just diplomats who act and gain specific knowledge, but experts who have to act, whether acknowledged or not, in a diplomatic manner so as to ensure the positive intersection of interests between sovereign states. Speaking of the wider trend, Slaughter (2004) claimed that:
"Regulators are genuinely the new diplomats - on the front lines of issues that were once the exclusive preserve of domestic policy, but that now cannot be resolved by

national authorities alone. These new regulators must often work side by side with the 'old diplomats', the highly trained members of national foreign services who must tackle delicate issues of statecraft. But the world of ambassadors in diplomatic dress presenting their nations' views to one another on a select set of security and economic issues is gone" (Slaughter, 2004, p. 64).

This article defines and develops the concept of systemic governance diplomacy and applies it to cyberspace in order to paint the picture of an emerging diplomatic paradigm related not only to cooperation, but also competition which is increasingly viewed as a zero-sum game for security and economy.

THE CYBER GOVERNANCE FRAMEWORK

Keating et al (2014) highlighted the differences between government and governance. Government relates to effective decision making and policy implementation. Governance refers to the institutions, rules, procedures, cultures and organizations which provide the framework for decision making.

The paradigm of rapid technological development that has become a cliché among ordinary people and stakeholders, as well as among experts, is mostly a general rationalization of developments in one field which penetrates and intertwines with all of the others – not material science, propulsion or energy production, but informatization and its material layer)servers, communication links, processing capabilities etc.). The prior section mentioned the extraordinary growth of cyber as a cross-cutting issue which is having a transformative effect on all critical infrastructure systems.

This rapid growth in capacity fuels the development of new applications and promotes wider penetration of cyber for key roles such as communication, coordination and integration. However, the governance capacity of individual states varies, but even that of the greatest powers is disrupted by the borderless nature of cyberspace, which automatically hobbles efforts like "The Great Firewall of China". Governance is especially lagging when it comes to discrete new technologies, such as autonomous/unmanned vehicles, AI, quantum computing, Internet of Things, blockchain or 5G (Gehrke, 2020). The lack of coverage by existing governance mechanisms means that these areas feature significant freedom for visionaries and entrepreneurs, but also develop and propagate significant risks. These new technologies, especially, fly under the radar until some current event thrusts them into the limelight and turns them into the object of hastily adopted and negotiated policies with significant flaws and a lack of staying power in international governance. The initial spread of blockchain attests to this, with indifference on the part of the authorities being followed-up by knee-jerk attempts at regulation, only now starting to organically form into capable governance structures bringing together relevant stakeholders (Katina et al, 2019).

Figure 1 presents an estimation of the current global organizational system of governance on cyber issues.

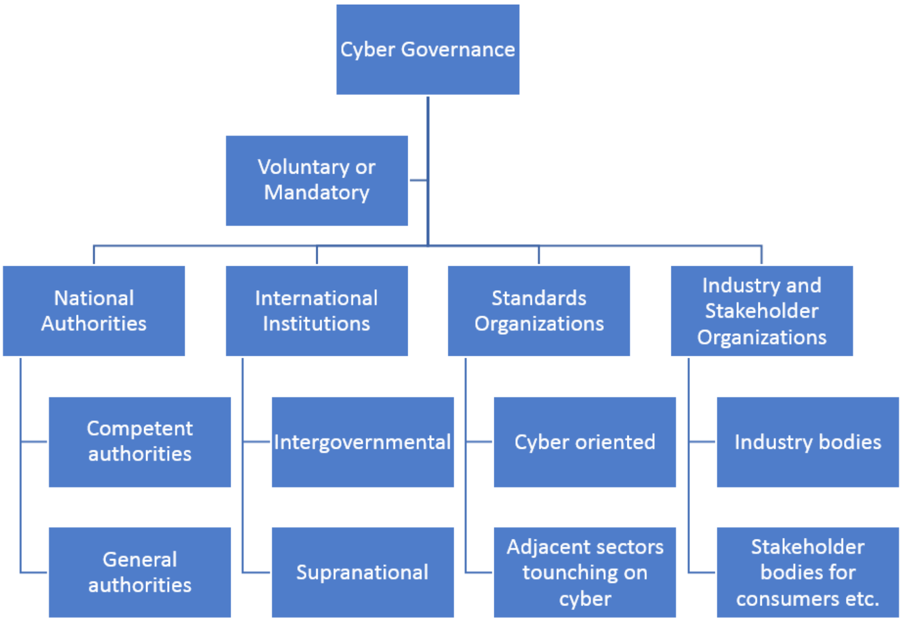


Figure 1. *The organizational framework for cyber governance issues (source: authors)*

We should highlight the diversity of governance stakeholders and the complexity of the resulting system, especially in a globalized and interconnected world. Of course, the mandatory\ voluntary dichotomy is a source of significant frictions and uncertainties (Georgescu et al, 2019), since some stakeholders may shirk responsibilities while others may use this system as a form of lawfare, to advance strategic interests other than safety, security and interoperability.

Figure 2 outlines the sources of framework of thought for governance activities on cyber issues, highlighting the diversity of sources and also the complexity of a system with binding and non-binding elements.

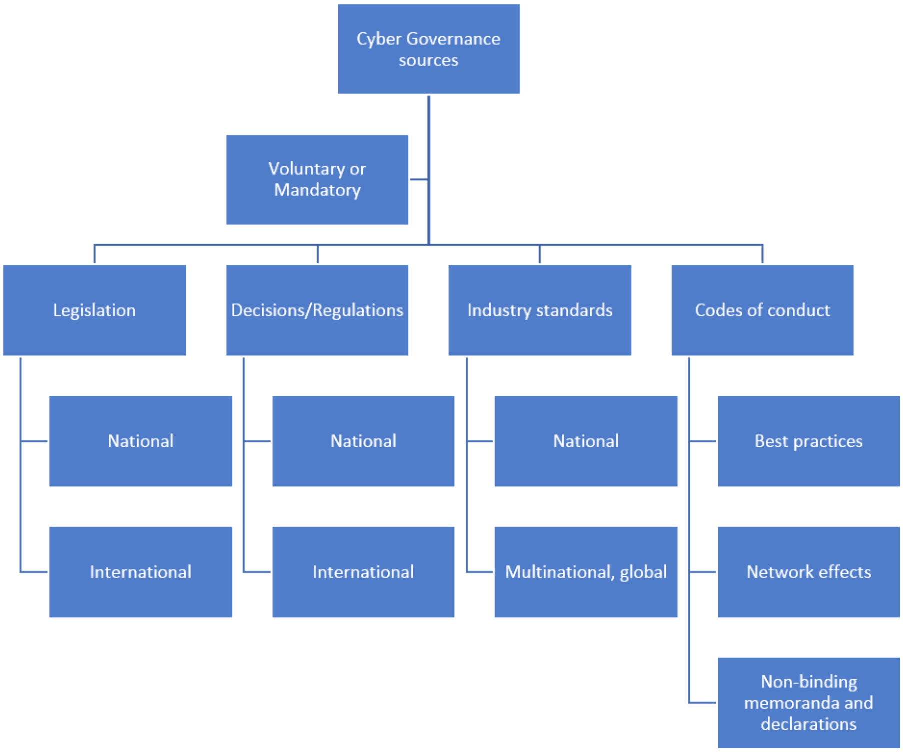


Figure 2. *The sources of policy and regulations for cyber governance issues (source: authors)*

The comments made for figure 1 are still valid for figure 2, and the legislative/administrative ecosystem is both continuously improving and permanently behind the curve, with overall security results likely to be hampered by the "weakest links" in an interdependent system, whether we are discussing nations like EU Member States or companies in a supply and production chain.

The issue of coordination among sovereign actors is crucial and can only be approached through diplomacy, with the exception of supranational regulation such as that provided by the EU. Even then, adoption and implementation are the object of continuous interaction, encouragement and prodding. The problem with ICT, as Bauer & van Eeten (2009) have underlined, is that a decentralized ICT system, whether we view it jurisdictionally or economically, will generate significant risk because of the externalities produced by security decisions on the part of individual stakeholders. Externalities are costs and benefits which are not registered by the actor who produces them. For instance, not supporting the cost of the insecurity produced by poor decision making (and, in a systemic sense, by poor regulation) results in negative externalities which diminish the ambient security of the entire system-of-systems (Bauer & van Eeten, 2009). The issue of "security decisions not properly reflecting social benefits and costs" can only be resolved through regulation, either of the activity or of the incentives of the stakeholders. While other models have been proposed, there still exists a spectrum of externalities which cannot be addressed by private action alone. But, given globalization, this regulation cannot stop at the borders, since countries already complain that the lower security standards of other countries are affecting their own security. It is diplomacy which can help bridge this divide – the various forms of diplomacy that are emerging and confirm that the need for specialized knowledge has led to the diplomatization of experts and the growth in expertise on the part of diplomats.

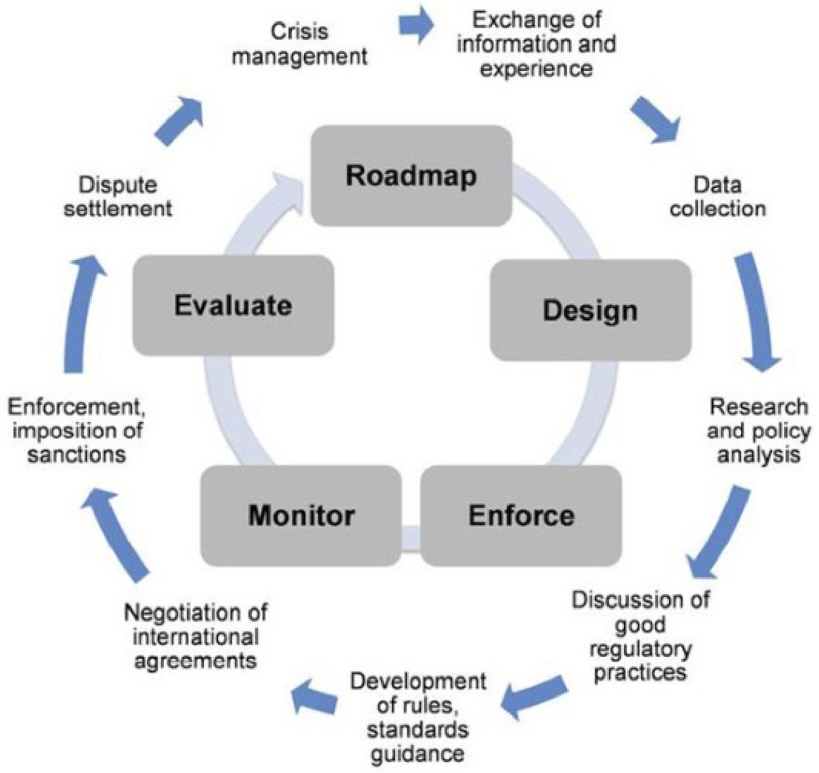

Crisis management
Exchange of information and experience
Data collection
Research and policy analysis
Discussion of good regulatory practices
Development of rules, standards guidance
Negotiation of international agreements
Enforcement, imposition of sanctions
Dispute settlement
Roadmap
Design
Enforce
Monitor
Evaluate

Figure 3. *Area of regulatory cooperation and the rulemaking cycle (source: OECD, 2016, p. 32)*

Figure 3 presents a generic cycle for international regulatory cooperation which is applicable to cyber and beyond and emphasizes the areas where activities related to diplomacy will take place, thereby emphasizing the internationalization of systemic governance in fields including cyber.

Table 1. *Forms of regulatory diplomacy also applicable to cyber*

Wiener and Alemanno (2015, p.111, apud OECD, 2012) recounted a non-exhaustive list of generic means for International Regulatory Coordination, which included:

1. Dialogue: informal exchanges for enhancing understanding of regulations;
2. Soft law: cooperation, in this case, is based on voluntary and non-binding instruments that encourage stakeholders to become involved in regulatory activities. In OECD parlance, these stakeholders are encouraged to notice and comment, provide input, and are given access to information, such as the OECD Guidelines and Principles;
3. Private codes: “Coordinated technical standards adopted by multinational private standards development organizations, such as transnational industry associations, or the International Organization for Standardization (ISO)” (Wiener and Alemanno, 2015, p.112);
4. Intergovernmental reliance on private codes, through the incorporation of existing regulations and standards into national legislation, such as ISO standards;
5. Trans-governmental networks: rather than develop formal treaties, networks bring together counterpart institutions and governmental units with regulatory importance in that respective sector and the cooperation advances through frequent contacts. The Basel Committee on Banking Supervision is one such example;
6. Mutual recognition agreements in national regulatory law, where national standards remain in force, but are considered roughly equivalent so that approval by one regulator automatically leads to approval by the other in order to access the latter’s market;
7. Regional and international agreements which aim to reduce regulatory barriers often end up adopting harmonized regulations. The World Trade Organization is an example, the North American Free Trade Agreement and, should they have entered into force, the Trans Pacific Partnership and the Transatlantic Trade and Investment Partnership;
8. Being a member of international organization can result in states working together with the institution to develop and voluntarily adopt standards, as proven by the OECD, by the International Maritime Organization, the International Labor Organization and the International Civil Aviation Organization;
9. Countries often engage, nowadays, in regulatory partnerships based either on formal or informal mechanisms. A larger discussion features in the next section, but the United States has pursued this strategy with the EU, Canada and Mexico. Another example is that between Australia and New Zealand;
10. Integration or harmonization of regulations through supranational institutions or joint institutions. These are found in two variants – weak forms, where countries sign treaties that lead to a chosen standard being integrated in national legislation, and strong forms, where supranational regulations supersede national ones, such as in the EU or in federations like the United States;
11. Lastly, joint regulators represent a pooling of sovereignty and an act of trust. The EU has advanced the most in this regard, but other examples include the Joint Food Standards Australia and New Zealand Agency. Depending on perspective and case by case regulatory initiatives, other bodies or even ad-hoc cooperation mechanisms may become this.

The reason why stakeholders will tend to shirk security and coordination and are required to, at the very least, establish a baseline security standard, is that security has costs in multiple ways, and the tendency of all stakeholders is to minimize costs in favor of profits, functionality, efficiency etc. Bauer et al (2008) liken this to a prisoner's dilemma, where stakeholders are incentivized to defect in order to internalize the cost savings from negligence while externalizing the resulting insecurity, even though it will eventually affect them as well. At the same time, once the stakeholders have internalized the necessity of cybersecurity, we find that their globalized nature imposes the added cost of having to deal with heterogeneous regulation for each market, thereby increasing their costs. This is where specialized standards and harmonization come into play, levelling the playing field for different markets so that economic stakeholders can more readily focus on their core activities. Wienner & Alemanno (2015) note that regulatory variation may match local preferences, but a certain amount of convergence is almost always a net positive, both from multinational businesses and the gains from combating shared problems, whether environmental or in cybersecurity. While such homogenization may result in regulatory error and stoke tensions through regulatory mismatches, it also serves to reduce interjurisdictional spillovers and perverse regulatory competitions that general lead straight to the bottom in terms of security.

Table 1 presents a brief and limited overview of the possibilities for regulatory diplomacy, which are greatly applicable to cyber, but have emerged over the past few decades in response to other crises and vulnerabilities of globalization, such the governance of drugs, food, energy, finance and others, many of which are today mediated and coordinated by cyber systems.

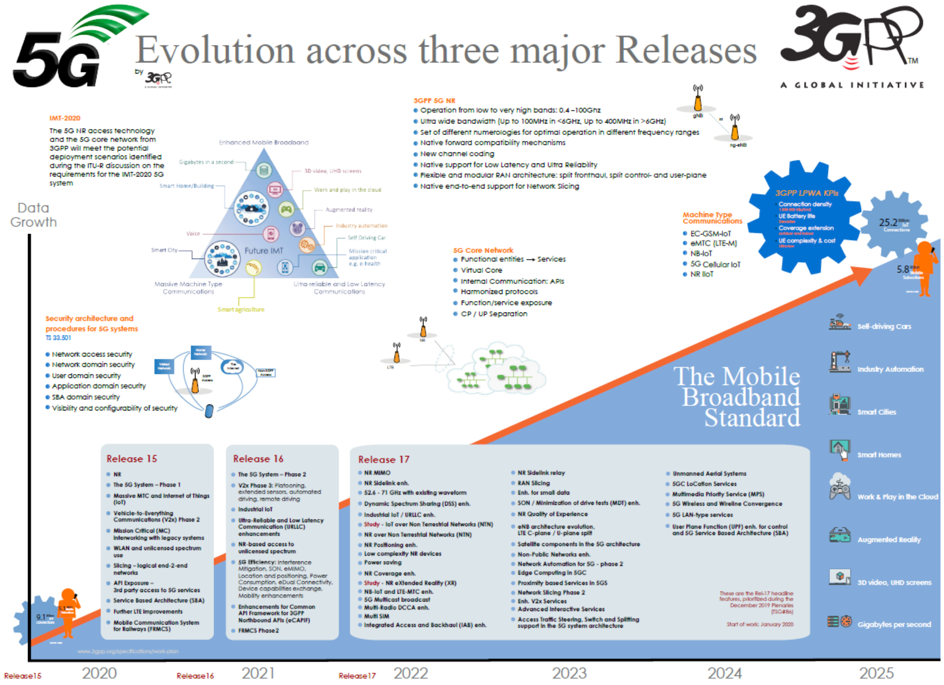
EXAMPLES OF SYSTEMIC GOVERNANCE DIPLOMACY

Gehrke (2020) emphasized overcoming the differences on trade policy in US-EU relations by including technology and security in the negotiations and widening the front of possible cooperation and trust building, to where the initial problem (that of trade) becomes surmountable through changes in the calculus of cooperation. He states that: "With U.S.-China technological competition a defining characteristic of this decade, a transatlantic technology cooperation agenda—addressing the rules, norms, and standards governing the use of emerging and sensitive technologies—is becoming a critical aspect of foreign policy and national security".

This is, of course, easier said than done, because it involves the next logical step in cooperation beyond the existing, already institutionalized one. One of the items on the agenda of the failed Transatlantic Trade and Investment Partnership was converging general regulation and standard setting, which was already difficult even before President Trump unilaterally terminated it. Golberg (2019) indicates diverging policy objectives, institutional set-ups, regulatory cultures, a lack of trust, and strategic competition as reasons for difficult regulatory harmonization negotiations, but this might as well describe all major actors, not just the US and EU, especially as they treat the area of standard setting as a theater for strategic competition.

One example of systemic governance diplomacy for cyber comes from the negotiations for Free Trade Agreements (Golberg, 2019). In order to set up the Comprehensive Economic and Trade Agreement with Canada, the EU and Canada pursued both horizontal and sectoral regulatory cooperation mechanisms. According to Golberg (2019), "the horizontal disciplines include good regulatory practices (publication of regulatory agendas, early information, public consultations, impact assessments, retrospective evaluations) and regulatory cooperation (enhancing compatibility of measures, preventing unnecessary barriers, exchanging information during regulatory cycle)". A Regulatory Cooperation Forum met for the first time in December 2018 and one of the five pillars of its action plan was cybersecurity and the Internet of Things. The Forum established thirteen committees and six specialized dialogues, some of which were inevitably dedicated to cyber issues. More and more of the EU's Free Trade Agreements will end up including provisions for regulatory cooperation on cyber, as the EU uses access to its market as an incentive for adoption of its preferred standards and for harmonization, leading to what Young (2015) termed as a potential "global regulator". The EU had, by 2019, 35 major free trade agreements with 62 partners (Golberg, 2019), and, since the 2006 "Global Europe" initiative, its FTAs have also focused on investment, services and regulatory issues, not just trade, with examples for South Korea, Singapore, Japan, Canada, Columbia-Peru and Central America. Of course, the entire domain of International Regulatory Cooperation is and will be applicable to cyber, either as general or sectoral regulatory harmonization. Both individual nations and bodies like the World Trade Organization view regulatory convergence as a factor for reducing trade and investment frictions.

Another area for systemic governance diplomacy is one that not only facilitates cooperation, but also competition – international standards initiatives and organizations, many of them organized as multilateral but by no means global initiatives. Examples in communications standards include the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the 3rd Generation Partnership Project (3GPP). As figure 4 points out, 3GPP is the most important for 5G standards.



5G Evolution across three major Releases by 3GPP

3GPP A GLOBAL INITIATIVE

IMT-2020

The 5G NR access technology and the 5G core network from 3GPP will meet the potential deployment scenarios identified during the ITU-R discussion on the requirements for the IMT-2020 5G system

3GPP 5G NR

- Operation from low to very high bands: 0.4 –100Ghz
- Ultra wide bandwidth (Up to 100MHz in <6GHz, Up to 400MHz in >6GHz)
- Set of different numerologies for optimal operation in different frequency ranges
- Native forward compatibility mechanisms
- New channel coding
- Native support for Low Latency and Ultra Reliability
- Flexible and modular RAN architecture: split fronthaul, split control- and user-plane
- Native end-to-end support for Network Slicing

5G Core Network

- Functional entities → Services
- Virtual Core
- Internal Communication: APIs
- Harmonized protocols
- Function/service exposure
- CP / UP Separation

Machine Type Communications

- EC-GSM-IoT
- eMTC (LTE-M)
- NB-IoT
- 5G Cellular IoT
- NR IIoT

3GPP LPWA KPIs

- Connection density
- UE Battery life
- Coverage extension
- UE complexity & cost

Security architecture and procedures for 5G systems
TS 33.501

- Network access security
- Network domain security
- User domain security
- Application domain security
- SBA domain security
- Visibility and configurability of security

Release 15

- NR
- The 5G System – Phase 1
- Massive MTC and Internet of Things (IoT)
- Vehicle-to-Everything Communications (V2x) Phase 2
- Mission Critical (MC) interworking with legacy systems
- WLAN and unlicensed spectrum use
- Slicing – logical end-2-end networks
- API Exposure – 3rd party access to 5G services
- Service Based Architecture (SBA)
- Further LTE improvements
- Mobile Communication System for Railways (FRMCS)

Release 16

- The 5G System – Phase 2
- V2x Phase 3: Platooning, extended sensors, automated driving, remote driving
- Industrial IoT
- Ultra-Reliable and Low Latency Communication (URLLC) enhancements
- NR-based access to unlicensed spectrum
- 5G Efficiency: Interference Mitigation, SON, eMIMO, Location and positioning, Power Consumption, eDual Connectivity, Device capabilities exchange, Mobility enhancements
- Enhancements for Common API Framework for 3GPP Northbound APIs (eCAPIF)
- FRMCS Phase 2

Release 17

- NR MIMO
- NR Sidelink enh.
- 52.6 - 71 GHz with existing waveform
- Dynamic Spectrum Sharing (DSS) enh.
- Industrial IoT / URLLC enh.
- Study - IoT over Non Terrestrial Networks (NTN)
- NR over Non Terrestrial Networks (NTN)
- NR Positioning enh.
- Low complexity NR devices
- Power saving
- NR Coverage enh.
- Study - NR eXtended Reality (XR)
- NB-IoT and LTE-MTC enh.
- 5G Multicast broadcast
- Multi-Radio DCCA enh.
- Multi SIM
- Integrated Access and Backhaul (IAB) enh.
- NR Sidelink relay
- RAN Slicing
- Enh. for small data
- SON / Minimization of drive tests (MDT) enh.
- NR Quality of Experience
- eNB architecture evolution, LTE C-plane / U-plane split
- Satellite components in the 5G architecture
- Non-Public Networks enh.
- Network Automation for 5G - phase 2
- Edge Computing in 5GC
- Proximity based Services in 5GS
- Network Slicing Phase 2
- Enh. V2x Services
- Advanced Interactive Services
- Access Traffic Steering, Switch and Splitting support in the 5G system architecture
- Unmanned Aerial Systems
- 5GC LoCation Services
- Multimedia Priority Service (MPS)
- 5G Wireless and Wireline Convergence
- 5G LAN-type services
- User Plane Function (UPF) enh. for control and 5G Service Based Architecture (SBA)

These are the Rel-17 headline features, prioritized during the December 2019 Plenaries (TSG#86)

Start of work: January 2020

www.3gpp.org/specifications/work-plan

Figure 4. *3rd Generation Partnership Project and the evolution of its 5G standard (sources: 3GPP, 2020)*

The Executive Working Group established after the meeting between President Donald Trump and then-President of the European Commission Jean-Claude Juncker in 2018 also tried to pursue cooperation on standards (including cybersecurity), in the vein of the older US–European Commission High Level Regulatory Cooperation Forum, which was active between 2005 and 2012 (Golberg, 2019). The Progress Report on the Implementation of the EU-US Joint Statement of 25 July 2018 established cooperation on cyber-surveillance, dual use exports and coordination in dealing with third parties. Just as the National Institute for Standards and Technology in the US advocated, cooperation with Europe seems to be gearing up to combat China's move towards influencing and setting standards, which is the natural complement of its leading position in communications technology and assorted products. The geopolitical dimension of this rivalry is quite notable, and has driven new EU regulations and directives on foreign direct investment, takeovers of strategic assets (companies with technology), and a closer cooperation between the EU and the US. Gehrke (2020) notes that the NIST in the US and the JRC in the EU could coordinate their efforts in international standards bodies (ISO, IEC, 3GPP), but also between internal bodies such as ANSI (American National Standards Institute) and CEN (European Committee for Standardization, one of three European Standards Organizations, along with CENELEC in electronics and ETSI in telecommunications) (NIST, 2012).

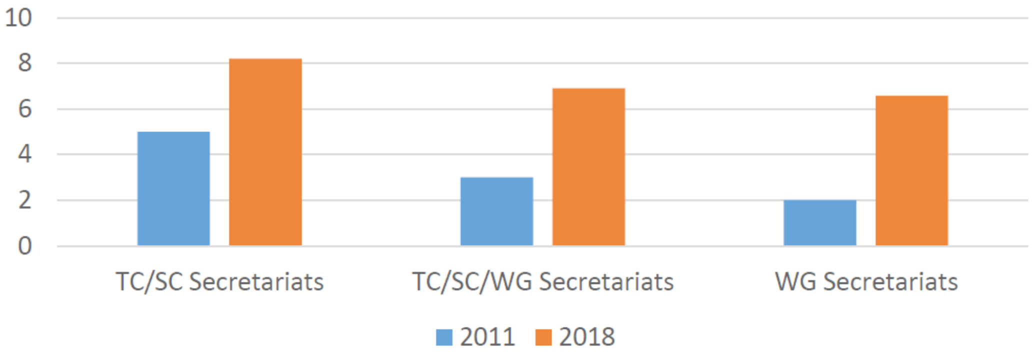


Figure 5. *China's share of Technical Committee secretariats, Sub Technical Committee secretariats and Working Group secretariats in 2011 and 2018 (%) for ISO (source: Fägersten & Rühlig, 2019, p. 10)*

Fägersten & Rühlig (2019) emphasize a strategy of standard setting on the part of China, with figure 5 showing the rapid growth in the presence of China in the various internal groups of the International Standards Organization. Kitson & Liew (2019) emphasized the strategic role of the Digital Silk Road in Chinese planning for globalizing companies, achieving leadership in technology and gaining market access, with 5G being just one facet of Chinese telecom dominance in the Belt and Road Initiative (BRI) countries:

- "Chinese telecoms equipment makers—including Huawei Technologies and ZTE—will play a prominent role in the launch of 5G networks across BRI member states";
- "Data centers and data storage infrastructure will continue to be built along BRI routes as China's communications providers look to position themselves in less-developed markets";
- "Chinese companies will seek to use the BRI as an opportunity to export their interpretation of smart city sensor and data platforms"

This, too, is a form of diplomacy, as is the use of initiatives such as the Belt and Road Initiative (though a Digital Silk Road), Made in China 2025, and the 5G technology\infrastructure export program to encourage adoption of preferred Chinese standards, technologies while also increasing market shares for Chinese companies.

CONCLUSION

Systemic governance is an unavoidable obligation on the part of governments and other stakeholders in the era of globalization and digitalization. We have created digital systems on whose functioning and performance we have come to rely for security, economic growth and socio-political processes. The scope of systemic governance goes beyond national jurisdictions and therefore must involve myriad forms of cooperation between sovereign states. This article has argued that cyber diplomacy is an important part of the process, as cyber is the cross-cutting domain/sector which connects most of the others, both functionally and in terms of the emergence and transmission of risks, vulnerabilities and threats. In the end, systemic governance is impossible without cyber, but sustainable cyber will be impossible without systemic governance in its field, whether it takes place through cooperative or competitive standard setting organization support, direct negotiations between governments or supranational cooperation, among other forms.

REFERENCE LIST

3rd Generation Partnership Project (2020) About 3GPP. https://www.3gpp.org/about-3gpp/about-3gpp

Bauer, J. M., van Eeten, M. (2009) Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy 33(10-11):706-719, https://www.researchgate.net/publication/227426674_Cybersecurity_Stakeholder_incentives_externalities_and_policy_options

Bauer, J. M., Van Eeten, M., Chattopadhyay, T., Wu, Y. (2008) Financial implications of network security: Malware and spam. Report for the International Telecommunication Union (ITU), Geneva, Switzerland, July 2008, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf

Fägersten, B., Rühlig, T. (2019) China's standard power and its geopolitical implications for Europe. Swedish Institute of International Affairs, February 2019, https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-brief-no.-2-2019.pdf

Gehrke, T. (2020) Transatlantic trade is stuck: time to integrate trade, technology and security, Commentaries, Royal Institute for International Relations, Egmont, 10 February 2020, http://www.egmontinstitute.be/transatlantic-trade-is-stuck-time-to-integrate-trade-technology-and-security/

Georgescu, A., Gheorghe, A., Piso, M.-I., Katina, P.F. (2019), "Critical Space Infrastructures: Risk, Resilience and Complexity", Topics in Safety, Risk, Reliability and Quality, Series 36, eBook ISBN 978-3-030-12604-9, DOI 10.1007/978-3-030-12604-9, Hardcover ISBN 978-3-030-12603-2, Series ISSN 1566-0443, Springer International Publishing

Golberg, E. (2019) Regulatory Cooperation – A Reality Check. M-RCBG Associate Working Paper Series No. 115, Mossavar-Rahmani Center for Business and Government, Harvard University, April 2019, https://www.hks.harvard.edu/centers/mrcbg/publications/awp/awp115

Katina, P. F., Keating, C. B., Sisti, J. A., Gheorghe, A. V. (2019) Blockchain governance. International Journal of Critical Infrastructures, 2019, vol. 15, issue 2, 121-135, http://www.inderscience.com/link.php?id=98835

Keating, C. B., Katina, P. F., & Bradley, J. M. (2014) Complex system governance: concept, challenges, and emerging research. International Journal of System of Systems Engineering, 5(3), 263–288

Kitson, A., Liew, K. (2019) China Doubles Down on Its Digital Silk Road. Center for Strategic and International Studies, 14 November 2019, https://reconnectingasia.csis.org/analysis/entries/china-doubles-down-its-digital-silk-road/

National Institute for Standards and Technology, Joint Research Centre (2012) The Benefits of U.S.-European Security Standardization. NISTIR 7861, June 2012, http://dx.doi.org/10.6028/NIST.IR.7861

Organisation for Economic Cooperation and Development (2016) International Regulatory Co-operation: The Role of International Organisations in Fostering Better Rules of Globalisation. OECD, 2016, ISBN 978-92-64-24404-7, DOI:https://dx.doi.org/10.1787/9789264244047-en

Slaughter, A. M. (2004) A New World Order. Princeton; Oxford: Princeton University Press. doi:10.2307/j.ctt7rqxg

Wiener, J. B., Alemanno, A. (2015) The Future of International Regulatory Cooperation: TTIP as a Learning Process Toward a Global Policy Laboratory. 78 Law and Contemporary Problems 103-136, https://scholarship.law.duke.edu/lcp/vol78/iss4/5

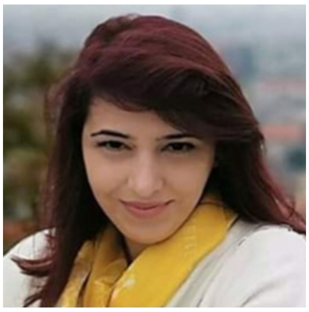
Young, A. R. (2015) The European Union as a global regulator? Context and comparison. Journal of European Public Policy 22(9), pp. 1233-1252, https://doi.org/10.1080/13501763.2015.1046902

Alexandru GEORGESCU

Is an Expert with the Department for Cybersecurity and Critical Infrastructure Protection of the National Institute for Research and Development in Informatics. He has an eclectic background, having studied Economics, then Geopolitics, and has obtained a PhD in Risk Engineering for Critical Infrastructure Systems. He is actively involved in advancing Critical Infrastructure Protection and Resilience issues through cooperation at international level and has worked on international projects for the European Space Agency, the Shanghai Institutes for International Studies and others. He is also affiliated with the European Center for Excellence for Blockchain, with the Romanian Association for Space Technology and Industry, the EURISC Foundation and Eurodefense. Coupled with significant International exposure, he is emerging as a notable member of a new generation of Romanian security experts.

Adrian Victor VEVERA

Is a Senior Researcher II, the Technical Director and a member of the Scientific Council of the National Institute for Research and Development in Informatics. Doctor of Military Sciences and Information, being both a lawyer and a nuclear physics engineer, Mr. Vevera has extensive experience in the field of national security, fulfilling various positions, over time, in numerous managerial and counseling positions in different state organisms. He has published numerous articles and papers on national and international security issues, energy security, cybercrime, critical infrastructure protection, and has been the coordinator of numerous projects of national interest.



Carmen Elena CÎRNU

Is Scientific Researcher II, Head of the Cyber Security and Critical Infrastructure R&D Department and Vice President of the Scientific Council at the National Institute for Research and Development in Informatics - ICI Bucharest, where she is involved in the development of research and development projects in the field of cybersecurity, cyber diplomacy, critical infrastructure protection and interoperability of e-government systems.

She graduated from the University of Bucharest in 2003, and obtained her PhD in 2011. An Aspen Institute Fellow and former Guest Researcher at Global Security Research Institute Japan, she held various roles in the research management area, as well as in the senior advisory area collaborating with universities and central public administration institutions over the years. She is the author or co-author of numerous articles, books, studies, and research reports and project manager for a significant number of national and international research projects in the field.