EU CYBERSPACE GOVERNANCE. WHICH WAY FORWARD?

Iulian F. POPA[1]

ABSTRACT

THE PURPOSE OF THIS PAPER IS TO FORMULATE A CONVINCING AND REALIST EXPLANATION CONCERNING A POSSIBLE FEASIBLE MODEL FOR GLOBAL GOVERNANCE OF CYBERSPACE AS THERE IS A CONTINUOUS DISAGREEMENT REGARDING THE ESTABLISHMENT OF NEW INTERNATIONAL RULES TO GOVERN THE CYBERSPACE, BOTH WITHIN AND OUTSIDE OF THE EU. FIRST AND FOREMOST THIS PAPER AIMS TO REVEAL THAT GOVERNANCE OF CYBERSPACE IS CRITICAL FOR THE NATION STATES AS THE COMPUTER NETWORKS ARE NOW ABLE TO TRANSCEND MODERN CONCEPTIONS OF TIME AND SPACE TO CHANGE THE POWER RELATIONSHIPS BETWEEN NATION STATES AND INDIVIDUALS. I ARGUE THAT THE GOVERNANCE OF CYBERSPACE HAS CONSIDERABLE CONSEQUENCES FOR NATIONAL SECURITY ALSO. LAST BUT NOT THE LEAST, THIS PAPER DRAWS THE ATTENTION TO THE EFFORTS MADE BY THE EU TO SECURE THE CYBERSPACE AS THE TRADITIONAL FORMS OF GOVERNANCE LACK IN CONTROLLING THE BORDERLESS CHALLENGES ENCOMPASSED BY THE INFORMATION AND COMMUNICATIONS TECHNOLOGIES.

KEYWORDS: CYBERSPACE, EUROPEAN UNION, CYBER GOVERNANCE, CYBER SECURITY

There is no academic consensus about what cyberspace really is. As Benjamin S. Buckland argues, the cyberspace *has many competing definitions*, mainly being defined as a broad network of huge ICT infrastructures[2] including Internet, telecommunications networks or SCADA computer systems in various industries. While a more formal agreement may never be reachable, both public and private actors around the world have shown a clear interest in defining the rules and best practices for behavior in cyberspace.

Therefore, for the purpose of this paper, I define the cyber governance as a method or system of government or management for the domain characterized *by the use of*

[1] Iulian F. POPA, M.A. is following a Ph.D. degree in Cyber Security and Defense at Babes-Bolyai University, Cluj-Napoca. E-mail: ifp2@georgetown.edu

[2]Look for more in Benjamin S. Buckland, Fred Schreier, and Theodor H. Winkler, *Democratic Governance Challenges of Cyber Security* (Geneva: DCAF Horizon, 2012).

electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures[3].

However, the last decade is characterized by the amazing growth of ICT which fosters continuously the progress of the human kind. The explosion in interoperability and functionality of the global Internet has undoubtedly redefined the way we think about traditional forms of governance.

While many scholars share different views about what cyber governance is, many agree that *the computer-generated public domain (cyberspace) has no territorial boundaries, is controlled by no single authority, it enables millions of people to communicate around the world* and maybe encourages threats to national security and internal governance stability of states[4]. As a consequence of the continuous emergence of ICT, the original purpose of the WWW (scientific data exchange, global economy support, freedom of information and communications, etc) has changed dramatically in the past decade. Consequently I argue that a feasible and broadly agreed cyber governance model is a must for states around the world. The first reason of such model is given by the fact that there are numerous ideological divergences in both our understanding of the issues and challenges, as well as in the technical and governance capabilities required to confront the threats to nation states. The second one is given by the previous ACTA (Anti-Counterfeiting Trade Agreement, 2011) experience which has shown to the world that we still face many democratic concerns about control, oversight and transparency of cyberspace governance[5].

Moreover, ACTA was considered an international overhasty agreement which was not modifying the substantive intellectual property rights law of the EU, and therefore does not imply any change to present EU laws. As a consequence, countries like Bulgaria, Czech Republic, Germany, Slovakia, and Slovenia are non-signatories or have indicated already to have stopped the process of its ratification. Moreover in February 2012, the European Commission asked the European Court of Justice to assess whether the ACTA agreement violates the EU's fundamental human rights and freedoms as there were great

[3] "Air Force Cyber Command Strategic Vision (unclassified)", US Air Force, accessed May 19, 2013, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479060.
[4] Brian D. Loader, *The Governance of Cyberspace: Politics, Technology and Global Restructuring* (London: Routledge, 1997), 12-30.
[5] Ronald Zittrain, John Deibert, Palfrey Rafal, and Jonathan Rohozinski, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press), 326-327.

debates over it. After being rejected by the European Parliament in July 2012, the European Commission has withdrawn ACTA referral to the European Court of Justice[6], and it became officially *fully dead within the EU*[7].

Today, when faced with both traditional and non-traditional challenges within the cyberspace and thus to national security, states tend to respond by promoting approaches based mainly on public private cooperation at all cyber governance levels. Therefore, in order to assure a chained interoperability, states acknowledge that these challenges entail the building of democratic cyber governance mechanisms for public private cooperation. Questioning this approach, Alyson Bailes points out that *cooperative cyber-governance becomes trickier to apply in an environment increasingly shaped by non-traditional, non-state, multinational or transnational forces and actors*[8].

Theoretically and technically, there are still unanswered questions yet. These questions are related to transparency, accountability, and costs of such cyber governance model as well as about ways it can contribute to improved security and risks mitigation. Currently we face many *gaps in our understanding of such complex governance networks* even though public and private actors are increasingly linked by versatile regulatory frameworks related to the electronic protection of critical infrastructure[9].

Despite the fact that public private cooperation has broadly shaped the concept of cyber governance and it has increasingly been the response to information age challenges, I agree with Alyson Bailes as I doubt this "ad-hoc" cyber governance model is enough to replace the traditional approaches, and to ensure full democratic oversight over cyberspace. In particular I believe that the globalized nature of governance networks complicates the issue from the perspective of transparency and control. As a consequence, my supposition is confirmed by the fact that democratic governance concerns related to cyberspace have never been more pressing as they are nowadays.

A number of things are clear from the above discussion. First, I consider that John Perry Barlow went too far by proclaiming the cyberspace as a *new libertarian virtual*

---

[6] "European Commission officially referred ACTA to the European Court of Justice", European Commission, last modified December. 2012, accessed May 21, 2013, http://trade.ec.europa.eu/doclib/press/index.cfm?id=799.

[7] "European Commission withdraws ACTA referral", *ACTA Blog*, December 20, 2012, http://acta.ffii.org/?p=1702.

[8] Look for more in Alyson Bailes "Private Sector, Public Security" in *Private Actors and Security Governance*, ed. Alan Bryden and Marina Caparini (Berlin: Lit Verlag).

[9] Idem 1.

world[10]. In my opinion, there is no doubt that cyberspace should be regulated by international laws as the online threats are emerging continuously. Combating these threats requires states *to look beyond the whole of government paradigm* and embrace, besides traditional approaches, effective and comprehensive public private cooperation mechanisms[11]. Second, within the EU and not only, the public private cooperation must involve, *not only the actors involved in so-called critical sectors, but also specialised internet security firms, software developers, hardware manufacturers, online payment providers, online content hosts, banks, financial sector actors, online commerce actors and private individuals* as Benjamin S. Buckland, Fred Schreier, and Theodor H. Winkler rightly point out.

EUROPEAN CROSS-BORDER STEPS TOWARD CYBER GOVERNANCE

Despite the willingness of many states to start the dialogue on international regulations for cyberspace, there is a continued disagreement on the new rules that are required to govern this 'new domain'[12], as Louise Arimatsu observes.

In the past few years, despite former and current controversies, global powers have decided to approach the issues of cyber governance by strengthening cooperation at both bilateral and international level, mainly because cyberspace is depicted as a domain of economic opportunity as well as of heightened risk. While many states are willing to cooperate, some still share fundamentally different legal perspectives: for example US considers primary threats as being the criminal ones rather than political ones, while Russian Federation is supporting the idea of state censorship and repressive domestic policies as best cyber governance practices, and so on. Even though there is a substantial expansion of the cyberspace and ICT in last decade, international security organizations along with law enforcement ones and private sector reached the consensus for a few times, despite appearances.

Besides other international efforts (mainly under the auspices of the United Nations and its partner organizations), within Europe first steps were made only in 2001, when the Council of Europe (CoE) adopted the Convention of Cybercrime Treaty (CoE-CCT). The

[10] "A Declaration of the Independence of Cyberspace", John Perry Barlow, accessed May 21, 2013, https://projects.eff.org/~barlow/Declaration-Final.html.
[11] Idem 1.
[12] Louise Arimatsu "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations" (paper presented at the 4th International Conference on Cyber Conflict, Tallin, June 4-7, 2012).

CoE-CCT was the first international agreement to tackle the cybercrime threats by international cooperation. The CCT encompasses common criminal policies within CoE members and harmonization of national computer crime laws along with law enforcement procedures. By adopting the Additional Protocol to the Convention on Cybercrime in November 2002, the CoE stressed the need for addressing the criminalization of racist and xenophobic acts too, committed through computer systems by extending of the Convention's scopes[13].

In December 2006, during the OSCE Ministerial Council Meeting, the Council passed the decision no. 7/06 - *Countering the Use of the Internet for Terrorist Purposes*, which called for states to expand international cooperation, take appropriate measures to protect critical infrastructures, increase monitoring of terrorist websites, and adopt the CoE Convention on Cybercrime[14].

Following OSCE's/CoE's initiatives, during the 2002 Prague Summit hold in Czech Republic, NATO initiated the establishment of the NATO Cyber Defense Programme and NATO Computer Incident Response Capability - Technical Centre (NCIRC TC) [15]. Furthermore, acknowledging the need for long-term cooperation in the protection of allied information systems, in the past years NATO established the allied Cyber Defense Concept along with the Cyber Defense Management Authority, and the Cyber Defense Center of Excellence located in Estonia. For such purposes, NATO maintains an online catalog of information security and information assurance products which is publicly available in its unclassified form[16].

In October 2005, under auspices of OECD, The Committee for Information, Computer, and Communications Policy (ICCP) during its forty-ninth meeting reported that *e-Government and the protection of national critical infrastructures appear to be two main drivers for developing a culture of security at the national level*. The report recommended the *adopting of a multidisciplinary and multi-stakeholder approach for establishing of a high-level governance structure which is necessary* for the implementation of national

[13] Michael A. Vatis, "The Council of Europe Convention on Cybercrime" (paper presented at *Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, DC, 2012)
[14] "Decision No. 7/06 Countering the Use of the Internet For Terrorist Purposes", Organization for Security and Co-operation in Europe - Ministerial Council, accessed May 20, 2013, http://www.osce.org/mc/23078.
[15] "NATO Rapid Reaction Team to fight cyber attack", NATO Newsroom, accessed May 19, 2013, http://www.nato.int/cps/en/natolive/news_85161.htm.
[16] "International Cyber Incidents – Legal Considerations", Eneken, Tikk et al., accessed May 19, 2013, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf.

cyber policies. In November 2012, OECD presented the *Cybersecurity Policy Making at a Turning Point - Analysing a New Generation of National Cybersecurity Strategies* report which stressed the fact that cyber security along with cyber governance are becoming national policy priorities in supporting of *economic and social prosperity cyberspace-reliant societies against cyber threats*[17].

Interpol, as a part of the international cyber governance mechanism, operates in Europe in case of cybercrimes that occur in more than one member country. The cybercrime division consists of the heads or experienced members of national computer crime units working in preventing and combating of cross-border threats and challenges to cyber security or cyber governance[18].

Within the European Union, following the joint efforts of Member States, European Network and Information Security Agency (ENISA) was created in 2004 by the **Regulation (EC) No 460/2004 of the European Parliament and of the Council. The main objective of the agency is to improve network and information security in European Union thus EU cyber governance, by** awareness-raising, supporting of communication between members, and data collection or prevention. ENISA is responsible for recording of all security incidents and emerging risks within EU and has a key role in coordinating Member States Computer Emergence Response Teams (CERTs). Also it assists the Commission, the Member States, and the business community in meeting the network and information security requirements and standards[19]. Along with the creation of ENISA, the European Commission has recognized the European Telecommunications Standards Institute (ETSI) as an European Standards Organization. ETSI is a main international cyber governance organization which *produces globally-applicable standards for Information and Communications Technology (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies*[20].

In order to provide a forum for exchanging experiences and knowledge and to promote common standards and procedures for responding to security incidents, a Task

[17] Look for more in Michael Portnoy and Seymour Goodman, *Global Initiatives to Secure the Cyberspace – An emerging landscape* (New York: Springer, 2009).
[18] "Fighting cybercrime worldwide requires law enforcement and private sector to work more closely together, says Interol Chief", Interpol – Media Release Centre, accessed May 18, 2013, http://www.interpol.int/News-and-media/News-media-releases/2013/PR043.
[19] "About Enisa – What does Enisa Do?", European Network Information and Security Agency, accessed May 20, 2013, http://www.enisa.europa.eu/about-enisa.
[20] "About ETSI". European Telecommunications Standards Institute, accessed May 22, 2013, http://www.etsi.org/about.

Force was established under the auspices of the Terena Technical Programme[21] to promote the collaboration between Computer Security Incident Response Teams (CSIRTs) in Europe. Informally known as TF-CSIRT, the Task Force provides a vehicle for CSIRTs in Europe to liaise with the European Commission and other policy making bodies.

Due to the fact that European Union is not yet positioning itself well enough to benefit from digital world developments, and therefore it *may be losing out in global competitiveness,* in December 2012 the European Commission adopted the Communication called "*The Digital Agenda for Europe - Driving European growth digitally'(COM(2012) 784*" which reveals the most important EU priorities on network and information security[22]. The document draws the attention on establishing a common minimum level of preparedness within the EU Member States and setting up cooperation mechanisms for mitigating and countering the threats and challenges within cyberspace. Following a feasibility study conducted by RAND Corporation – Europe, the European Commission decided to establish a European Cybercrime Centre (EC3) within Europol. The Centre is the main point in the EU's fight against cybercrime, contributing to faster reactions in the event of online threats and challenges. EC3 supports Member States and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners.

Starting 1 January 2013 EC3 commenced its activity under the auspices of Europol – the official European law enforcement agency, at the European Commission's special request. The main duties of EC3 focus on strategy and prevention to make European citizens and businesses much safer[23]. The EC3, in cooperation with Member States, monitors, analyses, and processes large amounts of data from a variety of sources to understand, strengthen, and mitigate the cyber threats within the European Union by operating 24/7. The need for such organization relies on the fact that today not all Member States have reached a satisfactory level of know-how required to effective fight against challenges to cyber security and governance.

---

[21] "Terena Technical Programme Update". Graf, Christoph, accessed May 22, 2013, http://www.terena.org/about/ga/ga36/TechnicalProgramme.pdf.

[22] "The Digital Agenda for Europe - Driving European growth digitally", European Commission, accessed May 22, 2013, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1381.

[23] "A Collective EU Response to Cyber Crime". Europol, accessed May 18, 2013, https://www.europol.europa.eu/ec3.

CONCLUSIONS

As like the security itself, the cyberspace is a very complex and important public asset. The governance of cyberspace, as a prerequisite of the information age, is still a relatively new topic, and there is no theoretical consensus about how it should look like. Harold Kwalwasser points out that the concept of cyber governance is a challenge to understand as no single actor dominates collective decision-making within cyberspace. The need for an adequate governance of cyberspace has shown that the traditional pillars of governance itself have changed radically in the last decade. As a consequence, the expansion of cyberspace *has not been accompanied by an adequate increase in security and governance*[24]. Joseph Nye argues that virtual communities freely expand across any offline territorial jurisdictions and develop their own patterns of governance while nation states become much less important to people's lives[25].

I agree that the global cyber governance lacks in regulation mechanisms and that may foster extreme behavior from citizens (hacktivist group called "Anonymous" is a famous example). At the moment, *the triangular relationship between states, companies – which are heavily present in cyberspace – and citizens – who use it massively – raises the issue of world [cyber] governance striking a new balance in order to respect the rights and interests of every actor*[26].

However, as Myriam Dunn Cavelty infers, like the governance of space and the oceans, the cyber governance requires globally accepted norms and regulation mechanisms. These are strongly required in order to mitigate and control the actual threats in cyberspace by creating *new and innovative ways to enhance protection of vital computer networks without inhibiting the public's ability to live and work with confidence on the internet*[27].

As regarding the European Union, many scholars draw the attention to the lack of cyber governance confidence among its citizens. For example, as the EU Directive 2006/24/EC on data retention was adopted by the European Parliament and the Council in March 2006, the public opinion within Member States seriously questioned the *libertarian*

[24] Look for more in Harold Kwalwasser, "Internet Governance" in *Cyberpower and National Security,* ed. Franklin D. Kramer, et al. (Washington, DC: National Defense University Press, 2009).
[25] Joseph Nye Jr., *Cyber Power* (Cambridge: Harvard Kennedy School, 2010), 12-25.
[26] Patrice Tromparent, "French Cyberdefence Policy" (paper presented at International Conference on Cyber Conflict, Tallin, June 4-7, 2012).
[27] Myriam Dunn Cavelty, "Unraveling the Stuxnet Effect: Of much Persistence and Little change in the Cyber Threats Debate", *Military and Strategic Affairs*, 3(2011):11.

nature of cyberspace and the respect for individual cyber freedoms within EU. In fact, the vast majority of public concerns arose due to the fact that *all member countries have to mandate the retention by telecom companies of the sender, recipient, and time of every Internet or other telecom communication*. Hence the above mentioned directive requires the collection and storage of all types of Internet Protocol identification data such as IP address, phone number, name or address of every online user, but the monitoring or storage of communications content itself it is not forbidden explicitly yet. As a consequence, starting April 2009, all Internet service providers within the European Union must strictly comply with all relevant national implementations of the directive[28].

As the cyber challenges and threats evolve continuously, I strongly believe that a cooperative cyber governance model is a major development opportunity for both public and private actors involved in prevention, mitigation, and response to cyber threats. Therefore I agree with the idea of Buckland, Schreier, and Winkler as I believe that full cooperation is crucial not only among the actors involved in critical sectors, but also among specialized internet security firms, software developers, hardware manufacturers, online payment providers, online content hosts, banks, financial sector actors, online commerce actors and private individuals.

Nevertheless I argue that every nation state should control the behavior of its citizens in cyberspace to guarantee the safety of the others. The law and cyber order should be enforced and continuously updated for best cyber governance practices. On the other hand, I strongly believe that the scope of any national governing mean, policymaking, law enforcement along with control and monitoring must fully comply with international law. Therefore any censorship practices against human rights must be strictly avoided by any actor confronted with cyber governance challenges.

[28] "Directive 2006/24/EC of the European Parliament and of The Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ", European Commission – Official Journal of the European Union, accessed May 19, 2013, http://eur-lex.europa.eu/.

REFERENCES

1. **ACTA Blog**, The. http://acta.ffii.org/?p=1702.
2. **Arimatsu, Louise** "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations." Paper Presented at 4th International Conference on Cyber Conflict, Tallin, June 4-7, 2012.
3. **Bailes, Alyson** "Private Sector, Public Security" in *Private Actors and Security Governance*, ed. Alan Bryden and Marina Caparini. (Berlin: Lit Verlag, 2006).
4. **Barlow, John Perry**. "A Declaration of the Independence of Cyberspace". Accessed May 21, 2013. https://projects.eff.org/~barlow/Declaration-Final.html.
5. **Buckland, Benjamin S., Fred Schreier, and Theodor H. Winkler**. "Democratic Governance Challenges of Cyber Security." in *DCAF Horizon* 1(2012):11-20. Accessed May 19, 2013. http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf.
6. **Dunn Cavelty, Myriam**. "Unraveling the Stuxnet Effect: Of much Persistence and Little change in the Cyber Threats Debate" *Military and Strategic Affairs*, vol. 3(2009): 11.
7. **European Commission** - Official Journal of the European Union. "Directive 2006/24/EC ". Accessed May 19, 2013. http://eur-lex.europa.eu/.
8. **European Commission**. "European Commission officially referred ACTA to the European Court of Justice". Accessed May 19, 2013. http://trade.ec.europa.eu/index.cfm?id=799.
9. **European Commission**. "EU Commission COM(2012) 784". Accessed May 19, 2013. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1381.
10. **ENISA**. "What does ENISA Do?". Accessed May 20, 2013. http://enisa.europa.eu/about.
11. **Europol**. "A Collective EU Response to Cyber Crime". Accessed May 18, 2013. https://www.europol.europa.eu/ec3.
12. **ETSI**. "About ETSI". Accessed May 19, 2013. http://www.etsi.org/about.
13. **Graf, Christoph**. "Terena Technical Programme Update". Accessed May 20, 2013. http://www.terena.org/about/ga/ga36/TechnicalProgramme.pdf.
14. **Interpol** – Media Release Centre. "Fighting cybercrime worldwide requires law enforcement and private sector to work more closely together, says Interpol Chief". Accessed May 18, 2013. http://www.interpol.int/News-and-media/News-media-releases/2013/PR043.
15. **Loader, Brian D**. *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. London: Routledge, 1997.
16. **Kwalwasser, Harold**. "Internet Governance" in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry. K. Wentz. Washington, DC: National Defense University Press, 2009.
17. **NATO Newsroom**."NATO Rapid Reaction Team to fight cyber attack". Accessed May 19, 2013. http://www.nato.int/cps/en/natolive/news_85161.htm.
18. **Nye, Joseph, Jr**. *Cyber Power*. Cambridge: Harvard Kennedy School, 2010.

19. **Portnoy, Michael, and Goodman, Seymour**. *Global Initiatives to Secure the Cyberspace – An emerging landscape*. New York: Springer, 2009.
20. **Tikk, Eneken, Kaska, Kadri, and Vihul, Liis**. "International Cyber Incidents – Legal Considerations". Accessed May 19, 2013. http://www.ccdcoe.org/publications/books/legalconsiderations.pdf
21. **Tromparent, Patrice**. "French Cyberdefence Policy." Paper presented at 4th International Conference on Cyber Conflict, Tallin, June 4-7, 2012.
22. **Vatis, Michael A**. "The Council of Europe Convention on Cybercrime" Paper presented at the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, Washington, DC, 2012.
23. **Zittrain, Ronald, John Deibert, Palfrey Rafal, and Jonathan Rohozinski**. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge: MIT Press, 2012.