The Global Regulation of Cybersecurity: A Fragmentation of Actors, Definitions and Norms

Tatiana Nascimento Heim* and Ramses A. Wessel**

Draft contribution to be published in Lucía Millán Moro (dir.) and Gloria Fernández Arribas (ed.), *Ciberataques y Ciberseguridad en la Escena Internacional*, 2020

1. Introduction

After the Second World War the international community agreed on a system of collective security. Decisions on the legal use of force were placed in the hands of the United Nations Security Council. These days, security threats are diverse. There is an increasing consensus that cyberthreats have become more frequent and that their result may have a similar disruptive effect on societies as the security threats the UN has in mind in 1945.[1] The modern state has adopted Information and Communication Technologies (ICT) as a tool to perform basic functions such as managing the economy, defense and, public health. Threats to ITC can harm the social and economic life of societies. Nowadays many states and individuals are living in a state of cyber-insecurity provoked by cyber-attacks, attacks on data privacy and other cyber threats that in most cases do not originate from states, but come from non-state actors and even individuals. Cyber-insecurity has a direct impact on society, leading to concerns about the social media, access to the web, spam, espionage, identity theft, viruses and freedom of expression.[2]

A recent example of cyber-insecurity is the event that occurred on October 7, 2016 when the Obama administration formally accused Russia of attempting to interfere in the US elections through launching cyberattacks[3]. Also, in June 2012, the New York Times reported that the United States and Israel developed the Stuxnet computer worm to attack an Irian computing system controlling the centrifuges use for uranium enrichment in order to prevent the country from manufacturing nuclear weapons.[4] In 2007, Estonia experienced an attack against government infrastructure, media and financial service that was termed a "digital Pearl Harbor"[5] placing NATO on high alert.

Furthermore, the internet is transnational in character and threats to its functioning cannot be regulated or dealt with by individual states, as state institutions have limited power control due to the de-territorial character of cyberspace. International law – and in a broader

* Doctoral Researcher, University of Twente, The Netherlands and lawyer at Zanella e Heim advocacia, Curitiba, Brazil

** Professor of International and European Law and Governance, University of Twente, The Netherlands

[1] CHOO, K., "The cyber threat landscape: Challenges and future research directions", *Computers & Security*, Vol. 30, 2011, num. 8, pp. 719-731.

[2] DE NARDIS, L., *The global war for internet governance*, Yale University Press, 2014

[3] HOSENBALL, M., VOLZ, D., LANDAY, J., "U.S. Formally accuses Russian hackers of political cyber attack. Reuters", Retrieved from: http://www.reuters.com/article/us-usacyber-russia-idUSKCN12729B (accessed 10.24.16).

[4] FIDLER, D. , "Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law", *American Society of International Law*, 2012.

[5] AAVIKSOO, J., "Cyberattacks against Estonia raised awareness of cyberthreats", *Defence Against Terrorism Review 3*, 2010, pp. 13-22.

sense international regulation – can provide tools for answering the questions related to opportunities to regulate the international cyber field. However, democracies and authoritarian / totalitarian states have varying perceptions about the internet and consequently about ideals of freedom of expression and access to information. Therefore, potential deals to maintain the peace require agreements on the balance of priorities with all of their political implications, while taking into account considerations of personal, corporate and national security.

Part of the difficulty to regulate cybersecurity relates to the actors who set rules and standards for cyber security. When the question of how to attain and maintain cybersecurity is raised, we are confronted with the fact that this area is not only (and perhaps not even primarily) governed and regulated by public (governmental) actors, but also by private (non-governmental) actors. Together, these measures and stakeholders create what may be called the 'internet security ecosystem'. In addition, this multi-actor dimension is complicated by the fact that governance and regulation take place in a multi-level (global, EU, national) setting in which different actors at different levels are responsible for many connected rules, standards and principles.

In this way, global governance of cybersecurity is formed by institutions and different kind of norms in a disorganized[6] and fragmented way.[7] The word fragmentation is commonly used to refer the proliferation of international regulations and the multiplication of international organizations.[8] Studies about fragmentation and international law usually argue that these phenomena can lead to conflicting norms,[9] forum-shopping,[10] overlapping jurisdiction[11] and legal uncertainty.[12] Fragmentation contributes to legal uncertainty as conflicting norms "reduce the predictability and reliability of law application".[13]

---

[6] LEVINSON, N., MERYEM, M., "International Organizations and Global Internet Governance: Interorganizational Architecture." *The Turn to Infrastructure in Internet Governance*, New York, 2016, pp. 47-71.

[7] NYE, J., "The regime complex for managing global cyber activities", *Global Commission on Internet Governance*, 2014; TROPINA, T., CALLANAN, C., "Self – and Co-regulation in Cybercrime, Cybersecurity and National Security", *Springer*, Heidelberg, 2015; COGBURN, D. "The Multiple Logics of Post-Snowden Restructuring of Internet Governance, " *The Turn to Infrastructure in Internet Governance*, Palgrave Macmillan, New York, 2016, pp. 25-45; LEVINSON, N., MARZOUKI, M., "International Organizations and Global Internet Governance: Interorganizational Architecture," *The Turn to Infrastructure in Internet Governance*, Palgrave Macmillan, New York, 2016, pp. 47-71.

[8] PROST, M. and CLARK, P. K., "Unity, diversity and the fragmentation of international law: how much does the multiplication of international organizations really matter?", *Chinese Journal of International Law*, 2006, pp. 341-370; KOSKENNIEMI, M., "Fragmentation of international law: difficulties arising from the diversification and expansion of international law: Report of the study group of the international law commission", 2014; HAFNER, G., "Pros and cons ensuing from fragmentation of international law." *Mich. J. Int'l L*, 2003; PAUWELYN, J., "Bridging fragmentation and unity: International Law as a universe of inter-connected islands", *Mich. J. Int'l L*, 2003.

[9] HAFNER, G., "Pros and cons ensuing from fragmentation of international law", *Mich. J. Int'l L*, 2003; PETERS, A., "The refinement of international law: From fragmentation to regime interaction and politicization", *International journal of constitutional law*, 2017, pp. 671-704.

[10] KOSKENNIEMI, M., "Fragmentation of international law: difficulties arising from the diversification and expansion of international law: Report of the study group of the international law commission.", 2014.

[11]KOSKENNIEMI, M. and PÄIVI, L., "Fragmentation of international law? Postmodern anxieties", *Leiden Journal of International Law*, 2002, pp. 553-579.

[12] KOSKENNIEMI, M., "Fragmentation of international law: difficulties arising from the diversification and expansion of international law: Report of the study group of the international law commission.", 2014; PETERS, A., "The refinement of international law: From fragmentation to regime interaction and politicization." *International journal of constitutional law*, 2017, pp. 671-704.

[13] PETERS, A., "The refinement of international law: From fragmentation to regime interaction and politicization." *International journal of constitutional law*, 2017, pp. 671-704.

In conclusion, there is a fragmentation of actors and norms of cybersecurity. This in turn led to a third type of fragmentation: definitions. The present paper aims to reveal and further analyze these three dimensions of fragmentation with the aim of finding possibilities to consolidate the global regulation of cybersecurity. The negative effect of fragmentation is that it leads to "frictions and contradictions between the various legal regulations"[14] and hence to legal and regulatory uncertainty. A positive side of fragmentation, however, is that it contributes to specialization and thus better reflects a particular situation. Fragmentation is therefore not simply 'bad'. As long as there is a workable consistency, "the rules coexist without conflicting with one another".[15] The final part of this paper will therefore look at possibilities for this coexistence, or perhaps even a consolidation of the fragmented norms.[16]

2. The Context: The Governance of Cybersecurity

Obviously, we are not the first in addressing the question of how to deal with the increasing cyber insecurity. Yet, existing literature mostly deals with various aspects of cybersecurity *governance* and less with a comprehensive view of global *regulation*. A first stream of literature sees cybersecurity governance as an extension of internet governance with a decentralized nature of stakeholders that address global cyberspace security and governance issues.[17] According to Nye, for instance, there are several regimes of governance of cyberspace formed by institutions, norms and regulations in a disorganized and fragmented way. The author argues that cybercrime and privacy are sub-issue susceptible to regime formation because of their importance in the information society.[18] In the same way, DeNardis understands the governance of cybersecurity as part of the governance of the internet, but emphasizes that "a question such as 'who should control de Internet, the United Nations or some other organization' makes no sense whatsoever. The appropriate question involves determining what the most effective form of governance is in each specific context".[19]

Cybersecurity governance is thus largely embedded in the study of internet governance. The Working Group of Internet Governance (WGIG) has defined internet governance as: "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmers that shape the evolution and use of the Internet." According to Kruger, there are two possible definitions of internet governance. The limited definition focus on the technological aspects of internet such as: domain names, standards, etc. The broader definition

---

[14] HAFNER, G., " Pros and cons ensuing from fragmentation of international law", *Mich. J. Int'l L.*, Vol. 25, 2003, pp. 849.

[15] D'ASPREMONT, J., "The systemic integration of international law by domestic courts: domestic judges as architects of the consistency of the international legal order" in NOLLKAEMPER, A, FAUCHALD, OK (eds.), *The Practice of International and National Courts and the (De-) Fragmentation of International Law*, Hart, 2012.

[16] VAN ASSELT, H., SINDICO, F., MEHLING, M., "Global climate change and the fragmentation of international law", *Law & Policy*, Vol. 30, 2008, num. 4, pp. 423-449.

[17] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism*, Vol.7, 2018, num.1 , pp. 112-141; JAYAWARDANE, S., *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance*, The Hague Institute for Global Justice Policy Brief, 2015; POWNER, D., "Cyberspace–US Faces Challenges in Addressing Global Cybersecurity and Governance." *Government Accountability Office*, 2010, num. GAO-10-606;

[18] NYE, J., "The regime complex for managing global cyber activities", *Global Commission on Internet Governance*, 2014.

[19] DE NARDIS, L., *The global war for internet governance*, Yale University Press, 2014

includes the policy related issues such as intellectual property rights, privacy, cybersecurity and commerce. The internet is by definition international and is governed by nation states and private sector stakeholders around the world.[20] Furthermore, in his book *Networks and States*, Milton Mueller explains that "Internet governance is the simplest, most direct, and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies."[21] The internet is a globally distributed computer network that includes interconnected autonomous networks. The type of governance is formed by a decentralized and multistakeholder international network, interconnected by autonomous groups, such as: civil society, the private sector, governments, academic communities, research organizations and national and international organizations.[22]

The clear link between internet governance and cybersecurity governance is not surprising. Also in conceptualizing internet governance it is common to use a multistakeholder model with the aim of improving structures and processes that reduce ambiguity, uncertainty and the immediacy of threats from unanticipated events.[23] In the cybersecurity multistakeholder model, each actor has different views of how the internet functions, which steps should be taken and what is actually meant by security in the internet.[24] Furthermore, the stakeholders have different degrees of power and influence in the cyberspace: "a constantly shifting balance of powers between private industry, international technical governance institutions, governments and civil society".[25] An important characteristic of the kind of governance that is dominant in cyberspace is that the relationships between stakeholders are informal and based on trust.[26] For example, in the cybersecurity field tech companies have much more strength and influence than States.[27] As Michael N. Schmitt and Sean Watts argue:

"Classically, states and non-state actors were differentiated not only by disparities in legal status, but also by significant imbalances in resources and capabilities. Not surprisingly, international law developed a state-centric bias to account for these imbalances. Cyberspace and cyber operations, however, have closed a number of formerly significant gaps between states' and non-state actors' abilities to compromise international peace and security. In fact, some non-state actors now match, if not exceed, the cyber capabilities of many states in this respect."[28]

For the present book, however, it is important to underline that the security dimension of internet governance is not only special, but also different for each of the stakeholders. The goal

---

[20] KRUGER, L., "Internet Governance and the Domain Name System: issues for congress", *Congressional Research Service*, 2013.
[21] MUELLER, M., *Networks and states: The global politics of Internet governance*, MIT press, 2010.
[22] LEVINSON, N., MARZOUKI, M., "Intergovernmental Organizations And Global Internet Governance Architecture", 2015.
[23] ADAMS, S., BROKX, M., DALLA CORTE, L., GALIC, M., KALA, K., KOOPS, B. J., ... and SKORVANEK, I, " The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK", *Tilburg University*, 2015.
[24] WOLFF, Josephine, "What we talk about when we talk about cybersecurity: Security in internet governance debates", *Internet Policy Review*, 2016.
[25] DENARDIS, L., *The global war for internet governance*, Yale University Press, 2014.
[26] MUELLER, M., *Networks and states: The global politics of Internet governance*, MIT press, 2010.
[27] BANNELIER, K., CHRISTAKIS, T. , "Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors", *Les Cahiers de la Revue Défense Nationale*, 2017, Paris, pp.11.
[28] SCHMITT, M., WATTS, S., "Beyond State-Centrism: International Law and Non-state Actors in Cyberspace", *Journal of Conflict and Security Law*, Vol. 21, 2016, num. 3, pp. 595-611.

of the private industry as one of the 'multistakeholders' in cybersecurity system is related to the proper functioning of the system (confidentiality, integrity and availability). [29] Furthermore, to prevent and combat the cyber threats the telecommunications companies and banks implement their own security measures.[30] Governments, on the other hand, focus more on the protection of values and the status quo;[31] their interest is to protect the critical information infrastructures and to keep the internet operational.[32] Meanwhile, civil society representatives are concerned about individual security, for example, privacy protection.[33] The citizen's focus in cybersecurity is on implementing firewalls and virus detection software on personal computers.[34] Together, these measures and stakeholders create what we have called the 'internet security ecosystem'. In short, the literature of cybersecurity governance frequently mentions the decentralized nature of the multistakeholders where each of the actors has a different roles and importance. This conclusion usually comes with the author's perception of this large plurality of international cyber-governance actors producing various international norms. This, as we will see, forms one of the key problems in attempt to regulate cybersecurity.

In addition, the multistakeholder model of cyber governance has led to a heterogeneity of cyber norms with different normative solutions for each problem.[35] Norms on cybersecurity can be found in national regulations, international law, technical protocols and standards, or political agreements; all involving substantial normative commitments in various stages of development and diffusion. The norms have a massive importance for cybersecurity governance because a significant number of rules about information security is lacking as result of the mistrust of legally binding agreements among nations. However, even if norms do not reach the status of international treaties they are part of the mentioned 'eco system' and they can help to develop a positive behavior among governments and ICT providers. In this way, the creation of norms is a first step to increase trust and they can eventually be rebuilt into international agreements.[36]

In conclusion, the global governance of cybersecurity architecture is thus characterized by a fragmentation that generates conflicting norms, forum-shopping and overlapping jurisdictions, leading to regulatory uncertainty.[37] Studies have shown that the global governance of cybersecurity reveals many stakeholders with different roles and different levels of importance in the system. These different roles and interests have, in turn, led to different understandings and definitions of cybersecurity. Finally, cybersecurity norms vary both in terms of their content and their nature; yet they are essential to increase trust between the

---

[29]WOLFF, Josephine, "What we talk about when we talk about cybersecurity: Security in internet governance debates," *Internet Policy Review,* Vol. 5, 2016, num.3.

[30] DE NARDIS, L., *The global war for internet governance*, Yale University Press, 2014.

[31] WOLFF, Josephine, "What we talk about when we talk about cybersecurity: Security in internet governance debates," *Internet Policy Review,* 2016.

[32] DE NARDIS, L., *The global war for internet governance*, Yale University Press, 2014.

[33] WOLFF, Josephine, "What we talk about when we talk about cybersecurity: Security in internet governance debates," *Internet Policy Review,* 2016.

[34] DE NARDIS, L., *The global war for internet governance*, Yale University Press, 2014.

[35] FINNEMORE, M., HOLLIS, D, "Constructing norms for global cybersecurity", *American Journal of International Law,* Vol. 110, 2016, num. 3, pp. 425-479.

[36] LEWIS, J., *Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms*. Center for Strategic & International Studies, 2014.

[37] PAUWELYN, J., "Bridging fragmentation and unity: International Law as a universe of inter-connected islands", *Mich. J. Int'l L.*, Vol. 25, 2003, pp. 903.

various actors. Our more legal institutional perspective aims to explain legal or regulatory uncertainty on the basis of these three forms of fragmentation: actors, definitions, and norms.

3. A Fragmentation of Actors

Stakeholders have different views about how the internet functions[38] and distinctive degrees of power and influence in cyberspace,[39] which leads to "a constantly shifting balance of powers between private industry, international technical governance institutions, governments and civil society".[40] For example, the goal of the private industry as one of the 'multistakeholders' in the cybersecurity system is related to the proper functioning of the system (confidentiality, integrity and availability).[41] Furthermore, to prevent and combat cyber threats, telecommunications companies and banks implement their own security measures.[42] Governments focus more on the protection of values and the status quo;[43] their interest is to protect the critical information infrastructures and to keep the internet operational.[44] Meanwhile, civil society representatives are concerned about individual security, for example, privacy protection.[45] The citizen's focus in cybersecurity is on implementing firewalls and virus detection software on personal computers.[46]

With a view to our aim to assess the global regulation of cybersecurity, we have limited our counting process to those acts that aim to play a role in the public governance of cybersecurity. A first mapping of these actors results in a stunning number, even if just we just count the main international actors. Our first analysis result in the following list (with reference to some literature): the European Union,[47] the Council of Europe,[48] the United Nations,[49] the

---

[38] DE NARDIS, *op.cit.*

[39] Ibid.

[40] Ibid.

[41] WOLFF, Josephine, "What we talk about when we talk about cybersecurity: Security in internet governance debates," *Internet Policy Review,* 2016.

[42] DE NARDIS, *op.cit.*

[43] WOLFF, Josephine, "What we talk about when we talk about cybersecurity: Security in internet governance debates," *Internet Policy Review,* 2016.

[44] DE NARDIS, *op.cit.*

[45] WOLFF, Josephine, "What we talk about when we talk about cybersecurity: Security in internet governance debates," *Internet Policy Review,* 2016.

[46] DENARDIS, L., *The global war for internet governance*, Yale University Press, 2014.

[47] WESSEL, R.A, "Cybersecurity in the European Union: Resilience through Regulation," in E. Conde Pérez (ed.), *Routledge Handbook of EU Security Law and Policy*, London/New York, Routledge, 2019; PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism,* Vol.7, 2018, num.1 , pp. 112-141; MUELLER, M., *Networks and states: The global politics of Internet governance*, MIT press, 2010; ORJI, U., *Cybersecurity Law and Regulation*, Wolf Legal, 2012; TROPINA, T., CALLANAN, C., *Self-and co-regulation in cybercrime, cybersecurity and national security*, Heidelberg, Springer, 2015; ODERMATT, J., *The European Union as a cybersecurity actor*. Research Handbook on EU Common Foreign and Security Policy**,** Steven Blockmans, 2018; ADAMS, S., BROKX, M., DALLA CORTE, L., GALIC, M., KALA, K., KOOPS, B. J., ... and SKORVANEK, I, " The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK", *Tilburg University,* 2015; BENDIEK, A., PORTER, A., "European cyber security policy within a global multistakeholder structure", *European Foreign Affairs Review*, Vol. 18, 2013, num. 2, pp. 155-180.

[48] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism,* Vol.7, 2018, num.1 , pp. 112-141; ORJI, U., *Cybersecurity Law and Regulation*, Wolf Legal, 2012; MUELLER, M., *Networks and states: The global politics of Internet governance*, MIT press, 2010.

[49] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism,* Vol.7, 2018, num.1 , pp. 112-141; ORJI, U., *Cybersecurity Law and Regulation*, Wolf Legal, 2012; JAYAWARDANE, S., LARIK, J., KAUL, M., "Governing Cyberspace: Building Confidence, Capacity and Consensus", *Global*

International Telecommunications Union (ITU),[50] the African Union,[51] Microsoft,[52] the Internet Engineering Task Force (IETF),[53] the International Organization for Standardization (ISO),[54] NATO,[55] Net Mundial,[56] the G7,[57] the Internet Governance Forum,[58] the Electrical and Electronic Engineers (IEEE),[59] the International Electro-technical Commission (IEC),[60] ICANN,[61] the Asia-Pacific Economic Cooperation (APEC),[62] the Organization for Security and

---

Policy, Vol. 7, 2016, n. 1, pp. 66-68; BENDIEK, A., PORTER, A., "European cyber security policy within a global multistakeholder structure", *European Foreign Affairs Review*, Vol. 18, 2013 n. 2, pp. 155-180; MACHADO, M., Cyber security governance: Securing the European Union´s Cyber Domain, 2015; MACLEAN, D., "Herding Schrödinger's cats: Some conceptual tools for thinking about internet governance", *Background Paper for the ITU WOrkshop on Internet Governance, Geneva February*, Vol. 26. 2004; BENDIEK, A., PORTER, A., "European cyber security policy within a global multistakeholder structure", *European Foreign Affairs Review*, Vol. 18, 2013, n. 2, pp. 155-180.

[50] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism*, Vol.7, 2018, num.1 , pp. 112-141; GUPTA, A.**,** SAMUEL, C., "A Comprehensive Approach to Internet Governance and Cybersecurity", *Strategic Analysis*, Vol. 38, 2014, n. 4, pp. 588-594.; ORJI, U., *Cybersecurity Law and Regulation*, Wolf Legal, 2012; JAYAWARDANE, S., LARIK, J., KAUL, M., "Governing Cyberspace: Building Confidence, Capacity and Consensus", *Global Policy*, Vol. 7, 2016, num. 1, pp. 66-68.

[51] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism*, Vol.7, 2018, num.1, pp. 112-141.

[52] Ibid.

[53] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism*, Vol.7, 2018, num.1 , pp. 112-141; GUPTA, A., SAMUEL, C., "A Comprehensive Approach to Internet Governance and Cybersecurity", *Strategic Analysis*, Vol. 38, 2014, num. 4, pp. 588-594; MACHADO, M., Cyber security governance: Securing the European Union´s Cyber Domain, 2015; MACLEAN, D., "Herding Schrödinger's cats: Some conceptual tools for thinking about internet governance", *Background Paper for the ITU WOrkshop on Internet Governance, Geneva February*, Vol. 26. 2004; MATHIASON, J., *Internet governance: The new frontier of global institutions*, Routledge, 2008.

[54] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism*, Vol.7, 2018, num.1 , pp. 112-141

[55] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism*, Vol.7, 2018, num.1 , pp. 112-141; ORJI, U., *Cybersecurity Law and Regulation*, Wolf Legal, 2012; ADAMS, S., BROKX, M., DALLA CORTE, L., GALIC, M., KALA, K., KOOPS, B. J., ... and SKORVANEK, I, " The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK", *Tilburg University*, 2015; DENARDIS, L., *The global war for internet governance*, Yale University Press, 2014; BENDIEK, A., PORTER, A., "European cyber security policy within a global multistakeholder structure", *European Foreign Affairs Review*, Vol. 18, 2013, num. 2, pp. 155-180.

[56] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism*, Vol.7, 2018, num.1, pp. 112-141; JAYAWARDANE, S., LARIK, J., JACKSON, E., "Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance", *The Hague Institute for Global Justice Policy Brief* , 2015.

[57] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism*, Vol.7, 2018, num.1, pp. 112-141.

[58] GUPTA, A., SAMUEL, C., "A Comprehensive Approach to Internet Governance and Cybersecurity", *Strategic Analysis*, Vol. 38, 2014, n. 4, pp. 588-594.; BENDIEK, A., PORTER, A., "European cyber security policy within a global multistakeholder structure", *European Foreign Affairs Review*, Vol. 18, 2013, num. 2, pp. 155-180.

[59] Ibid.

[60] Ibid.

[61] PERNICE, I., "Global cybersecurity governance: A constitutionalist analysis", *Global Constitutionalism*, Vol.7, 2018, num.1 , pp. 112-141; GUPTA, A., SAMUEL, C., "A Comprehensive Approach to Internet Governance and Cybersecurity", *Strategic Analysis*, Vol. 38, 2014, num. 4, pp. 588-594; JAYAWARDANE, S., LARIK, J., JACKSON, E., "Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance", *The Hague Institute for Global Justice Policy Brief* , 2015; MATHIASON, J., *Internet governance: The new frontier of global institutions*, Routledge, 2008; MUELLER, M., *Networks and states: The global politics of Internet governance*, MIT press, 2010; DREZNER, D., "The global governance of the Internet: Bringing the state back in", *Political Science Quarterly*, Vol. 119, 2004, num. 3, pp. 477-498.

[62] ORJI, U., *Cybersecurity Law and Regulation*, Wolf Legal, 2012.

Co-operation in Europe (OSCE),[63] the OECD,[64] the G8,[65] Interpol,[66] the organization of American States (OAS),[67] the Arab League and Gulf Cooperation Council,[68] the International Multilateral Partnership Against Cyber Threats,[69] the G20,[70] the Shanghai Cooperation Organisation,[71] the World Trade Organization (WTO),[72] the World Intellectual Property Organization (WIPO),[73] and UNESCO.[74]

This is what we mean by a fragmented actor structure. In line with how 'traditional' security was dealt with at the global level, one might have expected a particular role for the United Nations. Indeed, the UN does have an important role in the process of elaborating cybersecurity norms and it is being used as platform for States to fulfill their agendas.[75] For example the United Nations group of governmental experts (GGE) emphasis the need for: "dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure".[76] Yet, not even the UN has been able to function as a coordinating platform for the various actors that are active in the area.

4. A Fragmentation of Definitions

4.1 Defining cybersecurity

The plethora of actors with different contexts and different interest is part of the reasons why it has been quite difficult to reach consensus on definitions that are relevant in the cybersecurity domain. One may argue that this is not a problem as such, as long as actors in a certain arena agree on a common set of definitions. At the same time, the 'eco system' we described above, implies an increasing interconnectedness between these different arenas. They are partly overlapping and do not (and cannot) operate in isolation. The different actors, from government to business and citizens, are increasingly interdependent when it comes to finding workable solutions.

---

[63] BENDIEK, A., PORTER, A., "European cyber security policy within a global multistakeholder structure", *European Foreign Affairs Review*, Vol. 18, 2013, num. 2, pp. 155-180.

[64] ORJI, U., *Cybersecurity Law and Regulation*, Wolf Legal, 2012; MACLEAN, D., "Herding Schrödinger's cats: Some conceptual tools for thinking about internet governance", *Background Paper for the ITU WOrkshop on Internet Governance, Geneva February*, Vol. 26, 2004.
MACLEAN, D., "Herding Schrödinger's cats: Some conceptual tools for thinking about internet governance", *Background Paper for the ITU WOrkshop on Internet Governance, Geneva February*, Vol. 26. 2004 ; BENDIEK, A., PORTER, A., "European cyber security policy within a global multistakeholder structure", *European Foreign Affairs Review*, Vol. 18, 2013, num. 2, pp. 155-180.

[65] Ibid.

[66] Ibid.

[67] Ibid.

[68] Ibid.

[69] Ibid.

[70] BENDIEK, A., PORTER, A., "European cyber security policy within a global multistakeholder structure", *European Foreign Affairs Review*, Vol. 18, 2013, n. 2, pp. 155-180.

[71] Ibid.

[72] MACLEAN, D., "Herding Schrödinger's cats: Some conceptual tools for thinking about internet governance", *Background Paper for the ITU Workshop on Internet Governance, Geneva February*, Vol. 26. 2004.

[73] Ibid.

[74] Ibid.

[75] Ibid.

[76] United Nations General Assembly- Group of Governmental Experts on Developments in the Field of Information Telecommunications in the Context of Security, "A/65/201", http://www. unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf, 6.

Cybersecurity is an umbrella term that deals with security problems with a technical nature.[77] The term emerged from three main factors: the growing need of the society to use the internet as a tool to perform basic functions of the daily life; the existence of crimes and wars in society in general and the vulnerabilities of the internet.[78] There is a nomenclature problem about the term cybersecurity:[79] the use of the term depends on national priorities and policy implications and the context or purpose, and it can be spelled as 'cybersecurity' or 'cyber security' or cyber-security or even 'information security' (for this study we choose the most common spelling: 'cybersecurity'). Furthermore, the international community has different understandings of the meaning of cybersecurity and it can stand for different security concerns.[80] For example, China and Russia use the term 'information security' while the United States recognizes the term 'cybersecurity'. These differences of understanding and interpretations of the meaning and content of cybersecurity already make it difficult in principle to establish norms and rules of cyber conduct.[81] A computer system is secure when it can be trusted to behave as it expected to be. So, the traditional computer security concept is based on three elements: confidentiality, integrity, and availability. Confidentiality means that the information is accessible only for people authorized for it, integrity is related to the accuracy of the information and availability requires that the system is working without degradation.[82]

However, this concept has been criticized as incomplete and scholars added three more elements to the original concept: authentication, authorization and nonrepudiation. Authentication means verifying the source of a message or the identity of an individual. Authorization is what the user has permission to do. Nonrepudiation is proof to the sender that the data is sent to the real recipient and vice versa. In the same sense, the National Initiative for Cybersecurity (NICCS) glossary describes the concept of cybersecurity as: "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." [83] An alternative definition of cybersecurity is "the effort to protect information, communications, and technology from the harm caused either accidentally or intentionally".[84] The previous concept focus on the technical IT perspective but leaves aside the policies aspects, which are important because the impact of cybersecurity goes beyond the technological impact and involves government and policies. This is exemplified by the definition presented by Schatz (2017): "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber

---

[77] TROPINA, T., CALLANAN, C., *Self-and co-regulation in cybercrime, cybersecurity and national security*, Heidelberg, Springer, 2015.
[78] TABANSKY, L., *Cybersecurity in Israel*, Springer, 2015.
[79] CHOUCRI, N., DAW ELBAIT, G., MADNICK, S., "What is Cybersecurity?", *Explorations in Automated Knowledge Generation*, 2012.
[80] WEBER, R., STUDER, E., "Cybersecurity in the Internet of Things: Legal aspects", *Computer Law & Security Review*, Vol. 32, 2016, num. 5, pp. 715-728.
[81] KELLO, L., "The meaning of the cyber revolution: Perils to theory and statecraft. International Security", Vol. 38, 2013, num. 2, pp. 7-40.
[82] KUMAR, S., "Classification and detection of computer intrusions", Purdue University, 1995.
[83] CLARK, D., BERSON, T., LIN, H., *At the nexus of cybersecurity and public policy: Some basic concepts and issues*, National Academies Press, 2014.
[84] GUIORA, A., *Cybersecurity: Geopolitics, Law, and Policy*, Routledge, 2017.

environment and organization and assets."[85] This definition includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users.

In addition, it is possible to observe a trend between the literature that considered the main goal of cybersecurity as to protect information/data and information systems/infrastructure.[86] Thus, Ciolan explained cybersecurity as: "The protection of systems, but also the protection of data from alteration, corruption or deletion." On the other hand, part of the literature limits the goal of cybersecurity to the protection of information[87] that can be represented by the Australia Cybersecurity Strategy: "Are measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means."[88] Furthermore, Kissel and the New Zealand Cyber Security Strategy hold that cybersecurity is realigned with the protection of the cyberspace, and the Finland's Cyber Security Strategy argues that the concept aims at maintaining the safety of the cyber domain.[89]

States have also proposed definitions. The Cyber Security Strategy of Canada 2010, for instance, defines a cyberattack as: "Unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber-attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security".[90] This concept is narrower than the other ones but establishes the possibility of response depending on the severity of the cyberattack. However, it does not

---

[85] SCHATZ, D.,BASHROUSH, R., WALL, J. "Towards a more representative definition of cyber security", *Journal of Digital Forensics, Security and Law*, Vol. 12, 2017, num. 2, pp. 8.

[86] DUKES, C., "Committee on national security systems (CNSS) glossary", *CNSSI, Fort Meade, MD, USA, Tech. Rep*, Vol. 4009, 2015; DHS, A Glossary of Common Cybersecurity Terminology. National Department of Homeland Security, 2014, http://niccs.us-cert.gov/glossary#letter_c ; LEWIS, J., "Cybersecurity and critical infrastructure protection", *Center for Strategic and International Studies*, 2006; AMOROSO, E., *Cyber Security*, Silicon Press, 2006; CANONGIA, C., MANDARINO, R., "Cybersecurity: The new challenge of the information society", In: *Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions*, IGI Global, 2012, pp. 165-184; CAVELTY, M., "Cyber-security", *The routledge handbook of new security studies*, pp. 154-162, 2010; CIOLAN, I., "Defining Cybersecurity As The Security Issue of The Twenty First Century, A Constructivist Approach", *Revista de Administratie Publica si Politici Sociale*, Vol. 12, 2014, num. 1, pp. 40; HANSEN, L., NISSENBAUM, H., "Digital disaster, cyber security, and the Copenhagen School", *International studies quarterly*, Vol. 53, 2009, num. 4, pp. 1155-1175; SCHATZ, D., BASHROUSH, R., WALL, J., "Towards a more representative definition of cyber security", *Journal of Digital Forensics, Security and Law*, Vol. 12, 2017, num. 2, pp. 8.

[87] CYBER SECURITY STRATEGY, Office of the Attorney General, Australia, 2009, http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity#h2strategy; CANADA'S CYBER SECURITY STRATEGY, "For a Stronger and More Prosperous Canada", *Public Safety Canada/Sécurité publique Canada*, http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf, Oxford Online Dictionary, 2014, http://www.oxforddictionaries.com/definition/english/Cybersecurity h2strategy.

[88] CYBER SECURITY STRATEGY, Office of the Attorney General, http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity#h2strategy

[89] NEW ZEALAND'S CYBER SECURITY STRATEGY, http://www.med.govt.nz/upload/New%20Zealands%20Cyber%20Security%20Strategy%20Ju ne%202011.pdf; OXFORD ONLINE DICTIONARY, 2014, http://www.oxforddictionaries.com/definition/english/Cybersecurity h2strategy; Kissel, Richard, ed. *Glossary of key information security terms*, Diane Publishing, 2011; FINLAND'S CYBER SECURITY STRATEGY, 2013, https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

[90]; CANADA'S CYBER SECURITY STRATEGY, "For a Stronger and More Prosperous Canada", *Public Safety Canada/Sécurité publique Canada*, http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf

explain what severity of a cyberattack is and what is the potential response and mitigation could be. Hathaway added an element to the previous concepts that the purpose of the cyberattack has to be political or related to national security.[91] The political or national security purpose has the aim to differentiate cybercrime from cyberattack especially when the cyberattack is launched by a non-state actor.[92]

The authoritative Tallinn Manual established its own concept of cyberattack in Rule 30: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[93] The term cyber operation refers to military operations and activities using cyberattack,[94] and the definition relates to the fact that the Tallinn Manual aims to bring together the international legal rules that are applicable to cyber warfare. The latter is also clear in Rule 11: "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force".[95] Following the logic of the manual, the attack has to produce results similar to conventional weapons like death or destruction to be consider a cyberwar.[96]

In the same sense the lexicon of the US Cyber Command defined cyberattack as: "A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber-attack are not necessarily limited to the targeted computer systems or data themselves… A cyber-attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect."[97]

The key feature of these approaches is that they include that the attacks not only take place in cyberspace, but that they actually affect people and physical objects. The kinetic effect is usually an element to characterize the cyberattack as a cyberwar.[98] A cyberwarfare occurs when there is intend of causing damage, disruption[99] or destruction[100] of the adversaries' network and infrastructures with a political objective or the cyberattack cause severe consequences.[101] Following this definition, cyberwar "refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if

---

[91] HATHAWAY, Oona A, et al., "The law of cyber-attack", *Calif. L. Rev.*, Vol. 100, 2012, pp. 817.

[92] FAGA, H., "The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber attack, and cyber warfare in the 21st century", *Baltic Journal of Law & Politics*, Vol. 10, 2017, num. 1, pp. 1-34.

[93] SCHMITT, M., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

[94] LIN, H., "Offensive cyber operations and the use of force", *J. Nat'l Sec. L. & Pol'y*, Vol 4, 2010, pp. 63.

[95] SCHMITT, M., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

[96] PIPYROS, K. et al, "A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual", *Computers & Security*, Vol. 74, 2018, pp. 371-383.

[97] US DOD, "Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories – Joint Terminology for Cyberspace Operations", // http://www.nsci-va.org/CyberReferenceLib/2010-11- joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

[98] HATHAWAY, Oona A, et al., "The law of cyber-attack", *Calif. L. Rev.*, Vol. 100, 2012, pp. 817.; NYE JR, J., *Nuclear lessons for cyber security*, Air Univ Press Maxwell Afb Al, 2011.

[99] CLARKE, R., KNAKE, R., *Cyber war*, Tantor Media, 2014.

[100] KENNEY, M., "Cyber-terrorism in a post-stuxnet world", *Orbis*, Vol. 59, 2015, n.1, pp.111-128.

[101] FAGA, H., "The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber attack, and cyber warfare in the 21st century", *Baltic Journal of Law & Politics*, Vol. 10, 2017, num. 1, pp. 1-34.

not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to 'know' itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc".[102]

This approach comes close to is usually called 'information warfare' and "involves actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks".[103] Cyber warfare includes "any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system."[104] The term information warfare includes all techniques to disrupt or affect the information, for example, cyber attacks, cyberwarfare, and psychological operations. [105]

A second point that is worth noting, is that usually the actors that launch the cyberattack are nation states, international organizations[106] or political organizations and the targets are other countries "governmental and military information systems or at its commercial or infrastructure information systems for political purpose".[107] In other words, actions originating from an individual with personal motivations are not considered cyber warfare. In cyberwar the attacks are conducted during a time of crisis,[108] are coordinated by the governments (or other political organizations) and addressed to another country's governmental, military, and commercial or infrastructure system for political purpose.[109]

A final important type of cyberattack is cybercrime. Like the other concepts discussed, there is also no agreement on the concept of cybercrime,[110] but the concept is usually understood as an extension of existing criminal behavior[111] that uses different types of electronic devices to break the law.[112] Thus, electronic devices have to play a key role in the illegal practice.[113] Furthermore, cybercrime must violate existing national or international penal laws and the aim of the violation of the law is the profit gained by the attack.[114] Faga underlines that – in contrast to cyberwar – the concept of cybercrime "may only be committed by a non-state actor and must violate a state penal provision or international criminal law. The crime does not seek to

---

[102] ARQUILLA, J., RONFELDT, D., "Cyberwar is coming!", *Comparative Strategy*, Vol. 12, 1993, num. 2, pp. 141-165.
[103] HAENI, R., "Information warfare." *An Introduction. The George Washington University., Cyberspace Policy Institute, viewed*, Vol. 2, 2013.
[104] FORCE, US, *Cyber Warfare: A New Doctrine and Taxonomy*.
[105] MEHAN, J., "Cyberwar, cyberterror, cybercrime: a guide to the role of standards in an environment of change and danger", *IT Governance Ltd*, 2008.
[106] RAND CORP, "Cyber Warfare", http://www.rand.org/topics/cyber-warfare.html.
[107] DIPERT, R., "The ethics of cyberwarfare", *Journal of Military Ethics*, Vol. 9, 2010, num. 4, pp. 384-410.
[108] Ibid.
[109] Ibid.
[110] HATHAWAY, Oona A, et al., "The law of cyber-attack", *Calif. L. Rev.*, Vol. 100, 2012, pp. 817.
[111] TECHOPEDIA, "Definition of Cyberattack", www.techopedia.com/definition/24748/cyberattack; GORDON, S., FORD, R. "On the definition and classification of cybercrime", *Journal in Computer Virology*, Vol. 2, 2006, num. 1, pp. 13-20; MEHAN, J., "CyberWar, CyberTerror, CyberCrime and CyberActivism: An i-depth guide to the role of standards in the cybersecurity environment", *IT Governance Publishing*, 2014.
[112] MCQUADE III, S., "Encyclopedia of cybercrime**",** *ABC-CLIO*, 2008.
[113] GREATHOUSE, C., "Cyber war and strategic thought: Do the classic theorists still matter?", *Cyberspace and International Relations*, Springer, Berlin, Heidelberg, 2014, pp. 21-40.
[114] Ibid.

undermine the functions of a computer network, or possess a political or national security purpose".[115]

4.2 Defining cyber threats

A similar debate exists about the definition of cyber security *threats*. In the area of the Information Revolution, society has a wide and fast access to data and the possibility of processing and storing a huge amount of information. The term 'information' is meant to depict a coordinated set of data that is processed; its meaning is related to the perceptions and interpretations of the person who receives it.[116] A large amount of information also creates more intruders with skills and aim to harm the system and cause a large number of damages. The sophistication of the attacks has increased and technical knowledge can easily be acquired due to the fact that attack scripts and toolkits are available for beginners, with devastating effects for the society.[117] Any computer connected to the internet today is vulnerable to threats that cause financial losses that can range from minor errors to total system destruction.[118]

Cyber threats differ from traditional security issues mainly with regard to attribution and jurisdiction as a cyber-attack can be done from anywhere, without the actor leaving home. So, important security and law principles such as self-defense and armed attack that are based on territorial notions are not automatically applicable,[119] although attempts are made to apply existing rules to the cyberworld.[120] Threats to cyberspace can be classified in many ways and are often described differently by authors or organizations.[121] As demonstrated by the Cooperative Cyber Defence Centre of Excellence (CCDCOE) at the North Atlantic Treaty Organisation (NATO): "There are no common definitions for Cyber terms – they are understood to mean different things by different nations/organisations, despite prevalence in mainstream media and in national and international organisational statements."[122]

An early and important study about Computer Security Threat uses the term 'threat' as "the potential possibility of a deliberate unauthorized attempt to: Access information, manipulate information and render a system unreliable or unusable".[123] Threats to cybersecurity are difficult to classify because the different categories can overlap and the activities can

---

[115] FAGA, H., "The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber attack, and cyber warfare in the 21st century", *Baltic Journal of Law & Politics*, Vol. 10, 2017, num. 1, pp. 1-34.

[116] CAVELTY, Myriam Dunn. Cyber-security and threat politics: US efforts to secure the information age. Routledge, 2007.

[117] LIPSON, H., "Tracking and tracing cyber-attacks: Technical challenges and global policy issues", Carnegie-*Mellon Univ Pittsburgh Pa Software Engineering Inst*, 2002.

[118] ALHABEEB, M., et al. "Information security threats classification pyramid", *2010 IEEE 24th international conference on advanced information networking and applications workshops*, 2010, pp. 208-213.

[119] PERNICE, I., *Cybersecurity Governance: Making Cyberspace a Safer Place*, 2017.

[120] SCHMITT, M. (Ed.), *Tallinn manual on the international law applicable to cyber warfare*, Cambridge University Press, 2013.

[121] HANSMAN, S., HUNT, R., "A taxonomy of network and computer attacks", *Computers & Security*, Vol. 24, 2005, num. 1, pp. 31-43.

[122] NORTH ATLANTIC TREATY ORGANIZATION (NATO), "Cyber definitions" , https://ccdcoe.org/cyber-definitions.html.

[123]ANDERSON, J., "Computer security threat monitoring and surveillance", *Technical Report, James P. Anderson Company*, 1980.

originate from an individual actor or from a non-state actors and groups. For example, 'hacking' can originate from an organized crime, terrorist attack or a state aggression.[124]

The European Union's Cybersecurity Agency (formerly ENISA), understands cyber threats as a list of threats with information about threat agents and vectors that can lead to a loss or takeover of assets. In the environment of cyber threats, the assets in game change according to the scenario, users, and groups that are inserted as well as the patrimonial value of the threat.[125] Furthermore, cyber threats can also be considered security challenges that reach us through ICT equipment and networks that can be explored in a variety of illegitimate ways at different levels of aggression.[126]

At the same time, cyber threats may not only include deliberate attacks, but also other threats, such as unintentional disruption and outages caused by human error, environmental causes or technology failure. More generally, a study on *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses* divides cyberthreats in three categories: threat actors, threat tools and threat types. Threat tools are: "malware and its variants, such as (banking) Trojans, ransomware, point-of-sale malware, botnets and exploits"[127] and threat types are: "unauthorised access, destruction, disclosure, modification of information and denial of service".[128] Perhaps more accurately – also in view of the legal question of attribution[129] – the category of 'threat actors' can be rebranded to 'modalities of threats'. This category would then take into account the actors responsible for the attacks as well as their motivation.

Motivation indeed seems to be essential to find the applicable rules. The term cyberattack is often confused with the terms 'cyberwar', 'cybercrime', but the intend behind these threats obviously differs.[130] In this sense, Klimburg &Tirmaa-Klaar argue that: "cybercrime, cyberterrorism and cyberwarfare are often difficult to ascertain, and often lie in the eye of the beholder".[131] The term cyberattack is thus broad and used from simple computer attacks to full scale operations with the aim of wreaking physical destruction.[132] There are many different types of cyberattacks and the concept can be explained from different perspectives.[133] Taking a technical perspective, a cyberattack requires access to and exploitation of vulnerability and payload.[134] So, a cyberattack starts with the access of the attacker to the vulnerability of

---

[124] CORNISH, P., *Cyber security and politically, socially and religiously motivated cyber attacks*, 2009.
[125] MARINOS, L., SFAKIANAKIS, A., "Enisa threat landscape-responding to the evolving threat environment", *ENISA (The European Network and Information Security Agency)*, 2012.
[126] CORNISH, P., *Cyber security and politically, socially and religiously motivated cyber attacks*, 2009.
[127] VAN DER MEULEN, N., EUN, J., SOESANTO, S, "Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses", *European Parliament*, 2015, https://www.rand.org/pubs/research_reports/RR1354.html.
[128] Ibid.
[129] Ibid.
[130] FAGA, H., "The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber attack, and cyber warfare in the 21st century", *Baltic Journal of Law & Politics*, Vol. 10, 2017, num. 1, pp. 1-34.
[131] KLIMBURG, A., TIRMAA-KLAAR, H., "Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU", *European Parliament*, 2011.
[132] NYE JR, J., "Cyber power", *Harvard Univ Cambridge Ma Belfer Center For Science And International Affairs*, 2010.
[133] Ibid.
[134] NATIONAL RESEARCH COUNCIL, *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*, National Academies Press, 2009.

the system, followed by the exploitation of the vulnerability and at the payload stage things can be done "once vulnerability has been exploited".[135] In the payload stage cybersecurity is affected because there is a: loss of integrity, loss of availability, loss of confidentiality and physical destruction. Loss of integrity means that the data has to be protected from unintentional and improper modification. Loss of availability is when the system is unavailable to its users consequently affecting the functionality of the system and operational effectiveness. Finally, physical destruction means that the cyberattack creates physical harm.[136] Lin understands that the loss of confidentiality does not originate from cyberattacks but from cyberexploitations. Cyberexplotations, for this author, are attacks with the aim to obtain information that is confidential.[137]

From a multidisciplinary – that is: not merely technical – perspective the concept of cyberattack is often defined as to include: "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information resident in or transiting them".[138] Similarly, Randall argues that cyberattacks are a "large genus of all kind of attacks on information system. Such attacks include traditional counterespionage and disinformation campaigns, old-fashioned destruction of telephones lines, jamming of radio signals, killing of carrier pigeons"[139] Following this definition, the Technopedia dictionary has its own definition: "A cyber-attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft".[140] The concept emphasizes that the ultimate goal of cyberattack that is affecting the accuracy of the information.

5. A Fragmentation of Norms

It will not come as a surprise that the fragmentation of actors and definitions is related to a fragmentation of norms. One might argue that this is not a problem as long as there are no unsolvable conflicts of norms – for instance on the basis of rules of preference or hierarchy – and the norms merely apply in a certain arena (e.g. cyberwar or cybercrime) and in relation to certain actors. As we have seen, however, it is increasingly difficult to clearly separate the arenas and the relevant actors. There may be overlaps and even within one arena very different norms with a different legal nature may apply. As to the latter point, it is worth noting that the current regulatory framework can be seen as a patchwork[141] of soft and hard laws. And, as a result of the increasing mistrust of legally binding agreements among nations,[142] there is more

---

[135] Ibid.
[136] US ARMY CYBER OPERATIONS AND DOCTRINE COMMAND, "DCSINT Handbook No. 1.02", *US Army Tradoc*, Vol. 3, 2005.
[137] LIN, H., "Offensive cyber operations and the use of force", *J. Nat'l Sec. L. & Pol'y*, Vol. 4, 2010, pp. 63.
[138] LIN, H., "Lifting the veil on cyber offense", *IEEE Security & Privacy*, Vol. 7, 2009, num. 4, pp. 15-21.
[139] DIPERT, R., "The ethics of cyberwarfare", *Journal of Military Ethics*, Vol. 9, 2010, num. 4, pp. 384-410.
[140] TECHOPEDIA, "Definition of Cyberattack", www.techopedia.com/definition/24748/cyberattack.
[141] TROPINA, T., CALLANAN, C., *Self-and co-regulation in cybercrime, cybersecurity and national security*, Heidelberg, Springer, 2015.
[142] PAUWELYN, J., WESSEL, R., WOUTERS, J., "When structures become shackles: stagnation and dynamics in international lawmaking", *European Journal of International Law*, Vol. 25, 2014, n. 3, pp. 733-763.

soft law than hard law.[143] The existing legal norms do not provide a clear answer as to how states can respond to hostile cyber threats. [144]

The term hard law used in here refers to "legally binding obligations that are precise (or can be made precise through adjudication or the issuance of detailed regulations) and that delegate authority for interpreting and implementing the law".[145] This includes, for instance national regulations and international treaties. Soft law is a broad class which includes "soft obligations, (legal soft law), to non-binding or voluntary resolutions and codes of conduct formulated and accepted by international and regional organizations ('non-legal soft law'), to statements prepared by individuals in a non-governmental capacity, but which purport to lay down international principles.[146] In this contribution we use the wider definition (legal soft law and non-legal soft law) as to include different types of norms that are used to 'regulate' the security field. Examples include technical protocols[147] and standards,[148] political agreements, and public policy;[149] all involving substantial normative commitments in various stages of development and diffusion. The term 'norm' is used as standards of behavior defined in terms of rights and obligations.[150]

There are several cyber security norms distributed in different organizations and different levels. Norms that are frequently mentioned by the literature are those in the reports developed by the United Nations Group of Experts.[151] These reports developed an agenda for cybersecurity, confidence-building measures,[152] existing emerging threats,[153] and how international law applies to ICT.[154]

Furthermore, the Best Practice Forum (BPF), organized by the Internet Governance Forum, publishes reports with the aim of engaging the multistakeholders in cybersecurity policy matters.[155] The last edition of the forum establishes the importance of norms for cybersecurity: "The importance of norms as a mechanism in cybersecurity for state and non-state actors to agree on a responsible way to behave in cyberspace, given that the speed of legislation often struggles to keep up with the pace of changes in the sphere of cybersecurity."

---

[143] LEWIS, J., Liberty, *Equality, Connectivity: Transatlantic Cybersecurity Norms*, Center for Strategic & International Studies, 2014.
[144] SCHMITT, M., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.
[145]ABBOTT, K., SNIDAL, D., "Hard and soft law in international governance", *International organization*, Vol. 54, 2000, num. 3, pp. 421-456.
[146] CHINKIN, C., "The challenge of soft law: development and change in international law", *International & Comparative Law Quarterly*, Vol. 38, 1989, num. 4, pp. 850-866.
[147] LESSIG, L., *Code: And other laws of cyberspace*, ReadHowYouWant. com, 2009.
[148] MATHIASON, J., *Internet governance: The new frontier of global institutions*, Routledge, 2008.
[149] Ibid,
[150] KEOHANE, R., NYE, J., "Power and interdependence in the information age", *Foreign Aff.*, Vol. 77, 1998, pp. 81.
[151] SPIRITO, C., "Cyber norms for civilian nuclear power plants", *2016 International Conference on Cyber Conflict (CyCon US)*, IEEE, 2016.
[152] GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION TELECOMMUNICATIONS IN THE CONTEXT OF SECURITY, "A/65/201", https://undocs.org/A/65/201.
[153] GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION TELECOMMUNICATIONS IN THE CONTEXT OF SECURITY, "A/70/174", https://undocs.org/A/70/174.
[154] GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION TELECOMMUNICATIONS IN THE CONTEXT OF SECURITY, "A/68/98", https://undocs.org/A/68/98.
[155] IGF 2018 BEST PRACTICE FORUM ON CYBERSECURITY: CYBERSECURITY CULTURE, NORMS AND VALUES, http://www.intgovforum.org/multilingual/filedepot_download/6764/1437.

In the internet security governance system companies also have their role in developing norms. For example, Microsoft designed a Cybersecurity Policy Framework with the goal to influence policy-makers in the development of cybersecurity regulations.[156] At the national level, the Canada Cyber Security Strategy is often cited in the literature as a reference to the concept of cybersecurity.[157] This strategy was formulated in close cooperation with stakeholders. In the same sense, the United Kingdom National Cyber Security Centre coordinated a conference to discuss cyber norms with relevant companies.[158]

In addition to these more general strategies, certain more concrete norms and rules also are part of the patchwork of cybersecurity instruments. From the perspective of Africa, the continent developed the African Union's Cyber Security Convention and Personal Data Protection with the aim is: "defining the objectives and broad orientations of the Information Society in Africa and strengthening existing legislation on Information and Communication Technologies (ICTs) of Member States and the Regional Economic Communities (RECs)".[159] Recently, the European General Data Protection Regulation (GDPR) was adopted as an important regulation for data protection around the world.[160]

However, sometimes the rules or norms in the different instruments can be conflicting. For example, according to the Shanghai Cooperation Organisation's Information Security Agreement information war is: "mass psychologic[al] brainwashing to destabilize society and state, as well as to force the state to take decisions in the interest of an opposing party." [161] Furthermore, the Organisation understands the dissemination of information harmful to "social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other states" as one of the main threats to information security. [162] The Shangai Cooperation has an expansive vision of a cyberwar that "includes the use of cyber-technology to undermine political stability"[163]. At the same time, the Tallinn Manual – which aims to explain how international law applies to cyber operations – demonstrate a more restrictive view: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[164] The different visions about cyberwar form just an example of the various views on the same subject and the need for a clear definition of such an important problem. [165]

---

156 MICROSOFT, CYBERSECURITY POLICY FRAMEWORK, https://www.microsoft.com/en-us/cybersecurity/content-hub/cybersecurity-policy-framework.

157 ; CANADA'S CYBER SECURITY STRATEGY, "For a Stronger and More Prosperous Canada", *Public Safety Canada/Sécurité publique Canada*, http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf

158 HURWITZ, R., "Depleted trust in the cyber commons", *Air Univ Maxwell Afb Al Air Force Research Inst*, 2012.

159 AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

160 BUTTARELLI, G., "The EU GDPR as a clarion call for a new global digital gold standard" , *International Data Privacy Law*, Vol. 6, 2016, pp. 77–78 .

161SHANGHAI COOPERATION ORGANISATION'S INFORMATION SECURITY AGREEMENT, https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/SCO-090616-IISAgreement.pdf

162 Ibid.

163 HATHAWAY, Oona A, et al., "The law of cyber-attack", *Calif. L. Rev.*, Vol. 100, 2012, pp. 817.

164SCHMITT, M., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

165 HATHAWAY, Oona A, et al., "The law of cyber-attack", *Calif. L. Rev.*, Vol. 100, 2012, pp. 817.

Furthermore, the Tallinn Manual has a scale of effect approach that takes into account eight factors to assist states in understanding when a cyber-operation can be compared as a use of force. The problem of elaborating criteria is that there is always a chance of not being able to fill all forms of cyber threats. For example, the criteria of "invasiveness" are not compatible with the DDoS attack where the computer system is not infiltrated but there is an attempt to disrupt the traffic of the web property. Also, the majority of experts who formulated the Manual came from Western countries at the same time the rules are inspired by manuals of Canada, Germany, the United Kingdom, and the United States. Therefore, there is a fear that the Tallinn Manual is somewhat biased. [166]

Regarding cybercrime, in 2001, the Council of Europe elaborated the Budapest Convention on Cybercrime[167] that seeks international cooperation to harmonize legal enforcement against cybercrime. However, the convention does not authorize unilateral cross border searches, thus giving criminals more time to remove their traces. Furthermore, the time of the negotiation and drafting of the convention until the time that it was opened for signature took too long for a type of threat that is changing very fast. The problem of the lack of effectiveness added to the long process of negotiation resulted in increased demands from States for bilateral agreements, which in turn did not help to harmonise things.[168]

For example, in the European Union, the Cybercrime Convention was signed and ratified by a majority of countries but not by all of them, so even among EU Member States there is no common definition of cybercrime.[169] Furthermore, internally the European Union has Directives that also deal with cybercrime, but which use different definitions. Complexity is added when, for instance, the EU cooperates with other states, such as in the working group between the European Union and the United States that has as its goal to improve cyber incident management, public-private partnership, awareness-raising and cybercrime. This cooperation may conflict with the internal EU policies because: "it can be said that this internal rulemaking compares less than favourably with the EU's external rule-making, appearing instead piecemeal and less ambitious, in its failure to regulate holistically, transparently and systematically"[170].

In conclusion, the complexity of instruments about cybersecurity raises the question about their effectiveness, transparency and legal certainty. Much is being devised on the subject, but there is no organization and governance of the instruments and the actors.

6. Conclusion: From Fragmentation to Consolidation?

The main aim of this contribution was to address the complexities related to the global regulation of cybersecurity. These complexities mainly relate to the fragmentation of actors, definitions and norms. Cybersecurity as a field of public attention has developed rapidly over the past few decades. The piecemeal approach in which separate dimensions of cybersecuriy

---

[166] TANODOMDEJ, P., "The Tallinn Manuals and the Making of the International Law on Cyber Operations", *Masaryk University Journal of Law and Technology*, Vol. 13, 2019, num. 1, pp. 67-86.

[167]COUNCIL OF EUROPE, "*Convention on cybercrime",* num. 185, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

[168] GOLDSMITH, J., "Who controls the Internet? Illusions of a borderless world", *Strategic Direction*, 2007.

[169] FAHEY, E., "The EU's cybercrime and cyber-security rulemaking: mapping the internal and external dimensions of EU security", *European Journal of Risk Regulation*, Vol. 5, 2014, num. 1, pp. 46-60.

[170] Ibid.

were regulated has led to fragmentation. As argued above, fragmentation as such is not a bad thing as it also allows for special rules in special cases and situations. Yet, the further development of the internet and its possibilities have raised calls for a more consolidated approach, which would prevent possible conflicts between norms and would enhance legal certainty. With the many existing (public and private) actors and the many different instruments uses, it has become increasingly difficult to understand which norms are applicable in which situation. Moreover, the mentioned fragmentation has led to diverging rules in different countries and jurisdictions, making it more difficult for states to cooperate in a field that is by its nature 'borderless' and transnational.

While consolidation of the various instruments and norms is indeed difficult, it is not impossible to organize things differently. The European Union has recently done so when it rebranded its Agency for Network and Information Security (ENISA) to the European Union Agency for Cybersecurity, also with the idea to provide it with an overall coordinating role between the EU and its Member States.[171] While it is obviously easier to agree on this with 28 states, than with almost 200 globally, the time has come to start thinking about the global regulation of cybersecurity through a combination and perhaps consolidation of the different instruments. This is not going to be easy, but the many examples in the current contribution reveal that the current fragmentation is not the best way to face to cyber-insecurity we will most definitely face the coming decades.

[171] https://www.enisa.europa.eu.