Global Constitutionalism (2018), 7:1, 112–141 © *Cambridge University Press, 2018*
doi:10.1017/S2045381718000023

Global cybersecurity governance: A constitutionalist analysis

INGOLF PERNICE
Alexander von Humboldt Institute of Internet and Society, Französische Straße 9, 10117 Berlin, Germany

Email: pernice@hiig.de

Abstract: With the progressive digitisation and use, in particular, of the internet of things and artificial intelligence by industries, commerce, financial services, science and education, the public administration, health services as well as individuals, our society and daily life gets more and more dependent on the security of the net: cybersecurity. The new risks are self-made, a threat to almost everybody and new in kind. And they have a global dimension. For the difficulty of attribution of cyber attacks traditional concepts of deterrence and defence are not a solution. Given the new conditions of the 'digital constellation' this article aims at exploring instruments and methods of cybersecurity governance in a broad sense, learning from internet governance and taking a constitutional perspective. It is based upon shared responsibility, resilience and citizens' participation in the making and future application of an inclusive global rule-making system. Multi-stakeholder mechanisms are combined with deliberative processes, standardisation and legislative action. In accordance with the principles of global constitutionalism this new framework of global rule generation would emerge as a common democratic instrument of people to meet common challenges in addition and complementary to action for cybersecurity at the local, regional, national and supranational levels.

Keywords: cybersecurity; digitisation; internet governance; global constitutionalism; regulation

I. Introduction : Security in the digital constellation

Digitisation and the internet are changing our world, lives and society. They allow real-time business transactions and the functioning of financial markets worldwide. They provide quasi unlimited access to information, and allow real time communication beyond borders. Equal, safe and, preferably, free access to the internet is becoming a condition for everybody's participation in the markets, in social life and in politics. This includes access to culture, education and knowledge, to social networks and discussion platforms, to electronic markets and e-services. Open data

and e-government allow a new and closer relationship between citizens and public administration.[1]

The internet is also a medium of transparency, communication, participation and open public political discourse worldwide; frameworks, platforms and forums for open discursive processes of standard- and norm-setting on a multi-stakeholder basis are offered, as we already know from internet governance, and methods of e-democracy and e-voting based upon block-chain or other technologies are making political processes more inclusive and trustworthy. As outlined in another piece of work,[2] the internet even gives our imagination a perspective for developing a constitutional framework for commonly generated and accepted rules at the global level on issues requiring global regulation. Global constitutionalism[3] seems best to conceptualise the legal perspective of the process from which this framework may emerge, even in the absence of a *pouvoir constituant* in the traditional sense. It is about democratically legitimate procedures for taking decisions on issues that are beyond the reach of national politics and sovereignty. Common rules on the operation and use of the internet are just some of these issues, which also include policies against climate change and the preservation of peace and security worldwide. The digital revolution and the internet allow us to think beyond traditional limits of what constitutes the present world order, with a view to constitutionalising in a democratic way the so far fragmented system of international law and global governance.

Despite all its benefits, however, the digital revolution also has a flip side: cyber-attacks, new threats and risks for security, for data protection, privacy and other human rights. This is the 'dark side' of digitisation. The Snowden revelations have alarmed us about new forms of mass-surveillance by intelligence services, activities that have been perceived as an inacceptable threat to the privacy and freedom of people. Other attacks are directed against critical infrastructures, governmental institutions, private enterprises, and even hospitals and military systems. The ransomware attacks across many countries called WannaCry and NotPetya are but two examples of the publicly very visible cyber-attacks rolling around the globe.[4] In a speech of

[1] For the case of the European Union see I Pernice, 'E-*Government and E-Democracy: Overcoming Legitimacy Deficits in a Digital Europe*' in L Papadopoulou, I Pernice and JHH Weiler (eds), *Legitimacy Issues of the European Union in the Face of Crisis* (Nomos, Baden-Baden, 2017) 287.

[2] I Pernice, 'Global Constitutionalism and the Internet: Taking People Seriously' in R Hofmann and S Kadelbach (eds), *Law Beyond the State: Past and Futures* (Reihe des Frankfurter Exzellenzclusters, Campus-Verlag, Frankfurt am Main, 2016) 151.

[3] Ibid 176–84.

[4] See O Solon and A Hern, ''Petya' Ransomware Attack: What Is It and How Can It Be Stopped?' *The Guardian* (29 June 2017) at <https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how>.

14 February 2017, the German Minister of Research and Education said that the annual damage caused by cyber-attacks to German industry is estimated at 50 billion Euros.[5] The latest news has come from the German Ministry of Defence: they registered 284,000 cyber-attacks against IT equipment of the Bundeswehr during the first nine weeks of this year.[6] A new Cyber-Defence-Corps created this spring by the German government will consist of 13,500 IT-soldiers and specialists, and is supposed to grow further.[7]

The more governments become aware of the risks attending digitisation, such as cyber threats or foreign surveillance practices, the more often we hear calls for 'digital sovereignty'.[8] Yet, digital sovereignty, understood as an aspect of national sovereignty, is not the solution, at least as long as an open and free internet is regarded as beneficial to our societies. The internet, both with its benefits and risks, is borderless from the outset. There is nothing that seems to be more at odds with traditional concepts of state sovereignty, thus, than the internet. Neither individual states, nor even the international community have control over it. Given its rapid spread and popularity worldwide, substituting the internet by other technologies does not seem to be a realistic option. Nor have states an interest to cut themselves off or to establish their own system;[9] an alternative would not offer what the internet makes possible: global communication based upon a common technology (protocol).[10] One of the key conditions of its functioning, the domain name system, has developed in the form of, and is governed by a private corporation, ICANN, that has found recognition globally and was not in the past nor will it in future be controlled by one state.[11] In spite of

[5] J Wanka, Opening speech at the conference of 14 February 2017 on 'Selbstbestimmt und sicher in der digitalen Welt at <www.bmbf.de/de/selbstbestimmt-und-sicher-in-der-digitalen-welt-3906.html>.

[6] See Sputnik Europe of 3 April 2017, at <https://sputniknews.com/europe/201704031052246195-germany-military-cyberattacks-response/>.

[7] German Ministry of Defence, Press release of 30 March 2017: 'Bundesministerin der Verteidigung stellt neues Kommando Cyber- und Informationsraum auf' at <www.bmvg.de/resource/blob/10780/c868d16eae69008e936b6da227518020/30-03-17-bundesministerin-der-verteidigung-stellt-neues-kommando-cyber-und-informationsraum-auf-data.pdf>.

[8] Wanka (n 5).

[9] Regarding the case of China see J Goldsmith and T Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP, Oxford, 2006) 87–104, 183–4. See, on the other hand, M Mueller, *Will the Internet Fragment?* (Polity Press, Cambridge, 2017) 36–41, 60, 96–9.

[10] Mueller (n 9) 44–8, explaining this with the 'network effect'.

[11] For the development and elements of self-constitution see L Viellechner, *Transnationalisierung des Rechts* (Velbrück, Weilerswist, 2013) 128–43, 257–64. The originally established stewardship of the US government ended 1 October 2016, see ICANN Announcements of this date 'Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends' at <https://www.icann.org/news/announcement-2016-10-01-en>.

all attempts of states to taking over some control for their respective territory,[12] and in spite of the many tools developed for geo-blocking or content filtering with a view of protecting national intellectual property rights, public order[13] and, perhaps, in future even national democratic processes from foreign in information operations,[14] it is questionable whether national law and physical coercion will prevail, as suggested by Jack Goldsmith and Tim Wu in 2006 talking about 'the bordered Internet'.[15] What Milton Mueller rightly calls the '*mismatch* between its global scope and the *political and legal institutions* for responding to societal problems' (original emphasis),[16] as he argues, leads to more or less effective strategies of 'alignment', but not to a fragmentation of the internet.[17] National regulation and law enforcement regarding content, or data protection and privacy, for the protection of intellectual property, or the public order limits the use or even access to the internet, but accepts the internet as a global communication infrastructure. And with regard to cybersecurity even 'alignment' does not seem to be an effective tool against cyber-attacks from anywhere in the world.

With the increasing density of relations among people around the globe due to better information and communication, on the one side, and growing global challenges for which global response is required, on the other, and in spite of all divergencies regarding access to the internet, digital literacy and technological adaptation around the world, not to speak of the remaining 'digital divide', the digital society is becoming global step by step, and so must be governance and the regulation of the internet to protect public goods and ensure security in compliance with our common values.

[12] Goldsmith and Wu (n 9) 49–63 ('Why Geography Matters') and 65–85 ('How Governments Rule the Net').

[13] Regarding platform responsibility for criminal content on social networks see the 2017 German 'Netzdurchsetzungsgesetz' (Act to Improve Enforcement of the Law in Social Networks – BMJV), at <https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2>.

[14] With a warning: E Donahoe, 'Don't Undermine Democratic Values in the Name of Democracy' at <https://www.the-american-interest.com/2017/12/12/179079/>. For an initiative of China, Russia and others at the UN to establish an 'international code of conduct for information security' see Müller (n 9) 82, and the Letter dated 9 January 2015 (UNGA Doc A/69/723 of 13 January 2015), with an updated version of the draft. The Shanghai Cooperation Organisation continues discussing the initiative, see the SCO website at <http://eng.sectsco.org/news/20170204/209441.html>.

[15] This is the proposition of the very deep 2006 analysis of Goldsmith and Wu (n 9) 184.

[16] Mueller (n 9) 11, finding the mismatch between global cyberspace and the territorial state 'nowhere … more evident than in the domain of cybersecurity'.

[17] Ibid 71–104, concluding that even 'alignment is an illusion' (ibid 103–4).

Following some recent incidents of terrorism, Theresa May is calling for 'international agreements with allied democratic governments to regulate cyberspace to prevent the spread of extremist and terrorism planning'.[18] Yet, regulating the internet or cyberspace is not, as experiences shows, easily reached by international agreements. What is needed is, instead of digital sovereignty or international cooperation, a new global constitutional approach to governance and regulation, based upon digital competence, resilience and diligence, coupled with awareness of the risks of digitisation. What I would call the 'digital constellation', much more drastically than Jürgen Habermas' postnational constellation[19], is global; it is incompatible with the idea of national sovereignty and affecting the whole of (the globalised) society.[20]

Looking closer at cybersecurity, we discover that particularly in the world of security policies, digitisation has brought about dramatic structural changes. Traditional patterns need to be revisited. The following observations seek to highlight some of the characteristics to be borne in mind when assessing possible strategies of cybersecurity governance.

1. Cybersecurity is a concern of the individual user, and of businesses or undertakings at the micro-level, as much as of the society as a whole, states and supra- and international organisations at the macro-level. Communication and traffic systems, energy and water supply, even public services like education, health, police and government, can all be hit by cyber-attacks and cyber crime. We are, all of us, potential victims.
2. Similarly, all of us are potential attackers. The origin of threats to cybersecurity can be states, or governments, but also organisations, terrorist movements or individual hackers. One person alone can cause damage that in former times only an army or similar organisations were

[18] See J Stone, 'Theresa May says the internet must now be regulated following London Bridge terror attack' *Independent* (4 June 2017) with the explanation: 'We cannot allow this ideology the safe space it needs to breed – yet that is precisely what the internet, and the big companies that provide internet-based services provide, Ms May said', at <http://www.independent.co.uk/news/uk/politics/theresa-may-internet-regulated-london-bridge-terror-attack-google-facebook-whatsapp-borough-security-a7771896.html>.

[19] J Habermas, *The Postnational Constellation: Political Essays* (Polity Press, Cambridge, 2001).

[20] The term was coined by I Pernice, 'Risk Management in the Digital Constellation – A Constitutional Perspective', IDP Conference Barcelona (30 June 2017) HIIG Discussion Paper Series No. 2017-07, at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3051124> 10–14.

able to produce. Unknowingly and unwillingly, by using unprotected devices, all of us may even support DDos attacks or botnet actions.[21]

3. The quality and impact of cybersecurity threats range from the functioning of private IT-systems to the functioning of critical infrastructures of great geographical extent. Even nuclear plants and defence systems are not safe: if the entire electricity grid is hit for more than a short period of time, the entire system of communication and supply services risks breaking down. The result could be chaos.
4. The distinction between external and internal (cyber-)security policies has lost its meaning. Threats to cybersecurity can have external or internal, state or private, sources. As long as the problem of attribution remains unsolved, defence is a questionable concept and, in particular, cyber-deterrence or retribution and '*hack-back*' are not viable options.
5. The world of nation states as sovereign entities arranging their relations through international law is being challenged: a single state cannot govern even the essential conditions of security for its citizens on its own. The global scale of the internet with all its benefits, instead requires global mechanisms for protection against cyber-attacks, for setting up common rules and for ensuring law enforcement.

Talking about cybersecurity governance relates to aspects dealt with in the framework of internet governance, but with the focus on security it reaches in much broader issues of general policies. The recent impressive study by Karine Bannelier and Théodore Christakis, 'Cyber-Attacks – Prevention-Reactions' emphasises the 'extreme complexity of the problem, marked by the great diversity of the actors involved'.[22] Cybersecurity literature,

[21] For explanation of these terms see e.g. Digital Attack Map, 'What is a DDoS Attack?, at <https://www.digitalattackmap.com/understanding-ddos/>: 'A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources'; Techtarget, 'Botnet' at <http://searchsecurity.techtarget.com/definition/botnet>: 'The term *botnet* is derived from the words *robot* and *network*. A bot in this case is a device infected by malware, which then becomes part of a network, or net, of infected devices controlled by a single attacker or attack group'.

[22] K Bannelier and T Christakis, Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors, *Les Cahiers de la Revue Défense Nationale* (Paris 2017) 11: 'the extreme complexity of the problem, marked by the great diversity of the actors involved: potential perpetrators of cyber-attacks (States, ''proxies'', private actors supported or tolerated by States, terrorists, cybercriminals, companies conducting espionage or wanting to gain a competitive advantage, individual hackers, patriotic hacker groups, etc.); potential victims of attacks (States, administrations and communities, companies, media, individuals, etc.); those involved in these attacks (e.g. the States through which cyber-attacks transit, companies and individuals whose systems are used by the attackers without the knowledge of the owners); and, finally, those to be potentially involved in a response to a cyber-attack (States, private companies acting for their own benefits, private companies undertaking a response on behalf of another company, etc.)'.

so far, looks at specific incidents, instruments or legal questions. The aim of the present article is to take a broader perspective and relate the five observations made above to the question of governance, with a view to reducing this complexity. To this end, multilevel and, as an element of it, global constitutionalism is taken as a normative theory that informs and allows to frame a model of governance that includes legitimate rule-making at the global level as it would not be possible without the internet and, simultaneously, ensures that the internet itself is regulated and can be trusted as an communication infrastructure for not only economic but also democratic processes at all levels.

To be sure, the term 'governance' used in the present context is not identical with the term 'government'. It is understood in a broader sense and generally means the processes of coordination of behaviour in society by multiple actors and factors.[23] What emerges from governance, as a result, cannot be determined in advance. We can talk about governance even if there is not a single government acting, but many, and if there are other actors participating, like individuals, business enterprises, civil society organisations etc. This is what represents our present world order: our living conditions are emerging from a process in which state governments and many other actors and agencies are interacting, in the attempt also to manage critical moments, uncontrolled developments and factors that influence the human condition and behaviour.

One of these factors is the progressive use of IT and the internet. In parallel, there is an increasing threat to cybersecurity and trust, which are both, in turn, conditions for the application of these technologies. Cybersecurity governance encompasses all processes of coordination regarding cyberspace when new threats arise hand in hand with the adoption of new technologies and the introduction of new IT services for public and private use. Better understanding the specific threats and risks, their possible sources and our shared responsibility for cybersecurity and peace (section II) helps us better to assess the type of instruments available for preserving cybersecurity (section III). As it appears, the present toolbox fails to allow effective response to the increasing threats. Exploring some cornerstones of a system of cybersecurity governance in the light of global constitutionalism, however, seems to offer new perspectives for making cyberspace a safer place (section IV).

[23] For a conceptualisation of governance as 'flexible coordination' see J Hoffmann, C Katzenbach and K Gollatz, 'Between Coordination and Regulation: Finding the Governance in Internet Governance' (2016) *New Media & Society*, also at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836068> 19: 'Governance, we propose, should be defined as coordinating coordination or reflexive coordination, because it questions and potentially redefines the rules of the game.'

II. Assessing cyber threats and responsibilities

Threats to cybersecurity are a self-made evil in our society, an evil that seems to be spreading at the same speed at which applications of IT are increasingly determining our daily life. Cybersecurity threats differ from those involved in traditional security issues, in particular with regard to the problem of attribution. The risks we are taking thus compel us to revisit our notion of responsibility for the cyber threats we are facing as a result of adopting these new technologies.

Cyber threats – self-made evil

Today, there is no safe place in cyberspace. Cybersecurity policies have to seek effective protection for the individual as well as for the proper functioning of our economic, social and political systems. With the internet of things, we are becoming even more dependent, in matters of everyday life, on the security of the devices and services offered by IT and the internet. Smart homes and smart energy, electronic banking and financial markets, digital traffic regulation and autonomous cars, industry 4.0 or automated decision-making on taxation and in other fields of administration on their way to becoming 'smart government'[24] are but a few examples of applications through which we are making ourselves dependent upon functioning IT. In particular, the protection of critical infrastructures is key to the functioning of our societies, but so is the multitude of individually used hard- and software applications, machine learning and artificial intelligence that are increasingly determining our daily life and work.

We have allowed the internet in our digital society to play the role that oxygen plays in our daily life; stupidly, perhaps. The more we are dependent upon it, the more we have to take cybersecurity seriously. Before we become engaged in developing cyber armaments, however, with the effect of potentially increasing the threats to our security, it would seem to be

[24] For the concept see J von Lucke, 'Wie uns die intelligente Vernetzung zum Leitbild "Verwaltung 4.0" und einem smarten Regierungs- und Verwaltungshandeln führt' Whitepaper (14 September 2015) at <https://www.zu.de/institute/togi/assets/pdf/ZU-150914-SmartGovernment-V1.pdf>, and id, 'Deutschland auf dem Weg zum Smart Government – Was Staat und Verwaltung von der vierten industriellen Revolution, von Disruptionen, vom Internet der Dinge und dem Internet der Dienste zu erwarten haben' in (2016) *Verwaltung und Management* 171–86. M Flügge *et al*., 'Public IoT: Das Internet der Dinge im öffentlichen Raum' at <http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-4047629.pdf>. C Djeffal, 'Leitlinien der Verwaltungsnovation und das Internet der Dinge: Vom E-Government Zum Smart Government durch Verfassung, Gesetz, Organisation und Strategie' (Principles of Renewing Public Administration by the Internet of Things) (13 April 2017) at <https://ssrn.com/abstract=2952494>.

wise to better study and understand the risks. The first insight is the correlation between the increased use of IT and the increased risks we create, far beyond the IT systems *strictu sensu*. The more we make our societies dependent on safely functioning IT-related products, processes and structures, the more cybersecurity will be in demand.

Cyber defence and attribution

National security and defence policies, as we know from history, are directed against a potential or real enemy. The government of another country deciding to invade our country by sending troops and tanks, supported by naval and air forces may try to strike down our defences, walls, troops etc and to subject our country and people to foreign authority. Cyberwar and cyber-attacks are different. Nothing and nobody needs to move or invade; the attack works on the inside – simply through some signals or messages on the net from anywhere in the world – but the destructive effects can be similar. A cyber-attack might prepare the ground; it might be the first step followed by more classical warfare. It might be for other purposes. Who knows? And who knows where the attack is coming from? It could be a state, or an individual, or a terrorist organisation acting from within our own country or from outside it.

The problem of attribution remains unresolved.[25] In spite of great efforts – and some apparent success as in the case of the North Korean attack on Sony – there seems to be no technical solution to the problem yet.[26] Talking about 'cyber-deterrence' and 'self-defence' against a determined offender in the traditional sense, thus makes little sense, except cases where the attacker reveals reliably his or her identity. And even if we could qualify, legally, a cyber-attack of a certain gravity as an 'armed attack' in the sense of Chapter VII and, in particular, Article 51 of the UN Charter, who should we take measures to restore peace, or self-defence, against?

We thus need a conceptual change in security thinking. We also need to revisit our legal concepts and practical approaches to preserve international

[25] Industry representatives, though, claimed at the international conference titled 'Construire la paix et la sécurité internationales de la société numérique' at UNESCO in Paris on 6–7 April 2017 (<https://www.ssi.gouv.fr/uploads/2017/03/jesuisinternet-today_programme_20170404.pdf>) that the capabilities exist to technically retrieve the origin of a cyber-attack, but they would not give any names, for the offender may be their own client (some capability of this kind seems also to be behind the proposal of Microsoft, referred to in n 40 below).

[26] Private IT undertakings, however, claim that they are able to attribute cyber-attacks, and offer a public–private partnership. See the account by Bannelier and Christakis (n 22) 57–8, stating, however: 'this occult and informal "partnership" in attribution is, as it has been pointed out correctly, tenuous and even dangerous'.

peace and security in the digital constellation. This includes considering who is – or should be – responsible for the preservation of peace in the digital age.

Shared responsibilities for cybersecurity and peace

As everybody is a potential victim and a potential attacker in cyberspace, we find ourselves back in a Hobbesian 'state of nature'[27] – potentially a war of everybody against everybody. The answer of the contractualists in political philosophy was the social contract: the individual authorises the state to ensure security, if necessary by violence, while the state is bound to respect fundamental rights and constitutional principles like the democratic participation of the individual and the rule of law. Security, both internal and external, is the ultimate justification and responsibility of the sovereign state.

This was the approach during the seventeenth, eighteenth and nineteenth centuries. Eventually, terrible wars of the twentieth century told us that a new approach was needed. The idea of European integration, presented by Jean Monnet, can safely be taken as a revolutionary step ahead, giving us a period of almost 70 years of peace in the EU.[28] The new approach means that public authority is shared among diverse levels of responsibility for diverse areas of action, in accordance with the principle of subsidiarity. It adds new sovereign powers in areas that are beyond the reach of national policies. This seems to be the greatest achievement of political thinking in the twentieth century!

Similar creativity is needed in the twenty-first century for what I call the the digital constellation. States play a key role in preserving peace, but the digital constellation not only presents new opportunities, but also entails a new risk environment.[29] The responsibility of states includes what Bannelier and Christakis call 'cyber-diligence': protection against and prevention of cyber-attacks on and from the national territory.[30] But more is necessary. States are only one of the instruments available to help us organise cybersecurity and so preserve cyber peace – 'us' meaning the digital

[27] Interestingly, it is the renowned expert of constitutionalism Häberle who qualifies the 'spaces of the internet today as a partially law-free "status naturalis" to be developed into a "status culturalis"' (my translation); see P Häberle, 'Stichworte zum heutigen Konstitutionalismus – eine deutsche Sicht' in Häberle, *Vergleichende Verfassungstheorie und Verfassungspraxis. Letzte Schriften und Gespräche* (Duncker & Humblot, Berlin, 2016) 15, 25.

[28] I Pernice, 'European Constitutionalism and the Constitutions of the Member States. Implications for Brexit' (2017) Coimbra Faculty of Law Bulletin (available as: WHI-paper 01/2017).

[29] For the concept borrowing from Jürgen Habermas' concept of 'postnational constellation' see I Pernice, 'Risk Management in the Digital Constellation – A Constitutional Perspective' (2018) *IDP: Revista d'Internet, Dret i Política* (forthcoming).

[30] Bannelier and Christakis (n 22) 13, 16.

society, which is not national, not European or American, but is becoming global.

Is it possible to understand cybersecurity and peace not only as our common interest but, beyond this, as our shared responsibility? If we want to benefit from the new information technologies globally, can we excuse ourselves and escape from taking responsibility at this level? Thus, the question is: how can we conceptualise our shared responsibility for cybersecurity and peace at the global level? Let me offer an answer that is 'all inclusive': a multilevel and multi-stakeholder system of cybersecurity governance, a system that includes all stakeholders: the individual citizen and civil society, business enterprises, and public authorities, from the local up to the global level.

III. Ensuring cybersecurity and peace: The toolbox

Allocating responsibilities for cybersecurity to actors or institutions is one thing; the instruments for achieving cybersecurity and peace are another. This concerns the cybersecurity toolbox, with different roles for the diverse actors. While each of the tools is described separately hereafter, the perspective of cybersecurity governance implies that their interaction and synergies are what only can make them effective. The holistic approach conceptualising the diverse tools as part of one coherent system or strategy, with private actors and public authorities acting hand in hand, seems to enable achieving the necessary results.

Individuals: Self-protection, resilience, participation

As individuals and users of the internet, we cannot leave it up to only the public authorities to protect us. There is no such thing as an internet police force. Self-protection is necessary, possible and crucial. Self-protection in digital matters means education, digital literacy, care with our passwords, awareness and attention when we are purchasing and using hardware and software. Self-protection means the application of firewalls, regular updating of software, frequent backups, the responsible choice and use of devices, making sure that they are protected against, and not abused by hackers. Self-protection in some cases adds to the cybersecurity of others too.

Resilience is a priority. As a general concept 'resilience' means robustness as well as flexibility and adaptability.[31] It is about the quality of hardware and software. It may be costly but it pays off. Certain precautions, such as

[31] For a definition with more details see the Technical Report of the ITU-T Telecommunication Standardisation Sector of ITU, Focus Group on Smart Sustainable Cities (2/2015) 2, at <https://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx>.

updating software in order to increase robustness, can easily be taken by everybody. Regular backups allow the private user to protect themselves against the loss or destruction of documents or software.

In contrast, self-defence in the form of 'wild' hack-back[32] is not a tool applicable among private parties, if it is a tool at all. For deterrence, criminal law, and for compensation delict law exist and apply in cyber-relations as in other areas of personal security, without exception. But, again, how can we determine exactly who the attacker is?

An almost forgotten tool in the hands of the citizens is active participation in the political processes and multi-stakeholder bodies with the aim of enhancing cybersecurity. This includes discourse and pressure through civil society organisations, but also the use of information, transparency and control, made available by the internet, in order to press for more security and to hold political leaders and institutions accountable for their actions or omissions.

Business enterprises: Product design, alert systems, security-engineering, standards

Businesses should intensify efforts to support individual self-protection and to provide their own self-defence and security. No unprotected hardware device should be put on the market. Systems of bug detection and security updates for software should be mandatory. Enterprises have set up and should adhere to private systems for mutual information on cyber-attacks and sharing of best practices,[33] such as 'Threat-Exchange' offered by Facebook[34] and the German DCSO.[35] Such systems should stretch across borders and become global. Privacy- and security-engineering[36] must be part of the product development of all industries and have to be intensified. Technical standardisation in IT areas should focus also on privacy and security by design so as to meet basic security requirements.

As global players, private enterprises should proactively engage in the framing of structures to enhance cybersecurity. In some form of self-regulation they could establish globally applicable codes of conduct regarding privacy, data- and cyber-security and so set general standards for

[32] Discussing arguments pro and contra hack-backs: Bannelier and Christakis (n 22) 60–7. With regard to 'wild' hack-backs by private parties in particular see ibid 68–71.

[33] For recommendations to this effect of the US Department of Homeland Security see <https://ics-cert.us-cert.gov/Recommended-Practices>.

[34] See <https://developers.facebook.com/products/threat-exchange>.

[35] A start-up called Deutsche Cyber Sicherheitsorganisation; see <https://dcso.de/>.

[36] M Finneran Dennedy, J Fox and TR Finneran, 'The Privacy Engineer's Manifesto. Getting from Policy to Code to QA to Value' (2014) at <https://link.springer.com/book/10.1007%2F978-1-4302-6356-2>.

privacy- and security-engineering and establish technical safety requirements. A more audacious proposal is the trilogy of Microsoft with Brad Smith calling for the adoption of a 'Digital Geneva Convention to protect Cyberspace' as a legally binding instrument for states[37], supported by a 'Tech Accord' among business enterprises requiring them not to support 'offensive cyber operation', to protect customers, and to bolster first-response efforts.[38] The third pillar is the proposal to establish an 'Attribution Organisation' as a 'private-sector-led, independent and transparent' body to provide a 'foundation of a fact-based, global dialogue about the nature of significant cyber-attacks'.[39] The tasks of this organisation would be limited to attribution only, while incident response and enforcement would remain the responsibility of the states.[40] However, the establishment of such an organisation would presuppose that attribution is possible. No evidence, however, exists for this hypothesis.

Public authorities: Constitutional duties, European and international cooperation

States play a special role in cybersecurity. In a constitutional perspective, fundamental rights and principles are providing the framework for security policies: while limiting governments in their actions, they are also requiring legislators and governments to take action. The tools for public authorities at national, European and international level are diverse in impact and reach, ranging from awareness-raising and promoting best practices, legislation and the establishment of cybersecurity agencies, new forms of military defence, intelligence and intergovernmental cooperation, to cooperation within international organisations and through international treaties.[41]

Constitutional frame: Fundamental rights and principles

In 2008 the German Federal Constitutional Court established, in its famous case regarding online searches, a new fundamental right relating to cybersecurity:

[37] See the blog post of the speech of Brad Smith at <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0000pqr5pplgte46q5j12kemuejwn>. For the document see Microsoft, 'A Digital Geneva Convention to Protect Cyberspace' at <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH>.

[38] Microsoft, 'A Tech Accord to Protect People in Cyberspace at <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW6iCh>.

[39] Microsoft, 'An Attribution Organisation to Strengthen Trust Online' at <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI>.

[40] Ibid.

[41] For other instruments: Microsoft, 'Cybersecurity Policy for the Internet of Things' 13–17, at <https://mscorpmedia.azureedge.net/mscorpmedia/2017/05/IoT_WhitePaper_5_15_17.pdf>.

> The general right of personality (Article 2.1 in conjunction with Article 1.1 of the Basic Law [*Grundgesetz – GG*]) encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems.[42]

Fundamental rights protect the individual against public authority, and the Court found the right to integrity of information technology systems violated in the case on online searches.[43] But they are also an expression of values to be given effect by the legislator and may, thus, legitimise restrictions of other fundamental rights. This equally applies to Article 6 of the European Charter of Fundamental Rights, the guarantee of the 'right to liberty and security of the person', a wording similar to that of Article 5(1) ECHR. The ECJ understands the guarantee of the confidentiality and integrity of information technology systems as a full subjective right of the individual,[44] and refers to Article 6 of the Charter laying down 'the right of any person not only to liberty, but also to security', in order to emphasise, in its 2014 ruling on the case *Digital Rights Ireland*, that security constitutes an objective of general interest and, in particular,

> that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.[45]

The fundamental right to security so legitimises legislation that, within the limits of proportionality, imposes restrictions on other fundamental rights, like data protection. Given this broad interpretation, the right to security under Article 6 of the Charter means that if it is not a subjective right of the individual to be protected by the courts, at least it establishes a fundamental principle compelling governments and legislators to promote cybersecurity and to make sure that cybersecurity is taken seriously by businesses and individuals.[46]

Article 9(1) of the International Covenant on Civil and Political Rights (1966) providing for 'everyone … the right to liberty and security of

[42] Online-Durchsuchungen, judgment of 27 February 2008, BVerfGE 120, 274, English translation at <http://www.bverfg.de/e/rs20080227_1bvr037007en.html>.

[43] Ibid, paras 262ff.

[44] ECJ Judgment of 15 February 2016, case C-161/15 – PPU ECLI:EU:C:2016:84, paras 47–53.

[45] ECJ Judgment of 8 April 2014, cases C-293/12 and C-594/12 – Digital Rights Ireland and Others, EU:C:2014:238, para 44.

[46] For this interpretation see S Leuschner, *Vom Grundrecht zum Grundsatz. Sicherheit als Schutzgut der europäischen Grundrechtecharta – eine grundrechtsdogmatische Rekonstruktion und ihre Folgen für die Sicherheit im Cyberraum* (Mohr Siebeck, Tübingen, 2017). On positive obligations of states arising from the human rights in the ECHR see H Krieger,

person' should be interpreted in the same way: it compels states and organisations to take action on cybersecurity and, in implementing this duty, to engage in international cybersecurity cooperation.

Legislation and agencies

At a European and national level, one important focus of legislative activities is rules on general information, warning and cooperation requirements in the event of cyber-attacks. The EU's Agency for Network and Information Security (ENISA) was set up in as early as 2004, and since then has provided expertise and encouraged cooperation between national authorities. It is now responsible for supporting the implementation of the new Directive 2016/1148 'concerning measures for a high common level of security of network and information systems across the Union' (NIS). This Directive mainly provides for national cybersecurity strategies, cooperation and trust among national authorities within a 'computer security incident response teams network' ('CSIRTs network'). It also establishes security and notification requirements for operators of essential services and for digital service providers. It is to be transposed into national law by May 2018, though much of its contents is already in place in some Member States. In Germany the 'Federal Office for Information Security' (BSI) was established as early as 1991, and the new 'IT-Security Act' of 2016 largely implements the requirements of the Directive.[47]

Cyber crime is another area in which action has already been taken. The Treaty of Lisbon established a new competence of the EU to harmonise legislation on computer crime.[48] Directive 2013/40/EU on attacks against information systems is a first, but important, step to combat cyber crime and to protect cybersecurity EU-wide. Data security is mentioned as one of the principles of data protection under Article 5(1)f GDPR, and Articles 32 to 34 of this Regulation impose on the controllers and processors of data not only the duty to ensure security of the data in their possession but also to notify personal data breaches to the supervisory authority and to

'Positive Verpflichtungen unter der EMRK: Unentbehrliches Element einer gemeineuropäischen Grundrechtsdogmatik, leeres Versprechen oder Grenze der Justiziabilität?' in (2014) 74 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 187–213, also at <http://www.zaoerv.de/74_2014/74_2014_2_a_187_214.pdf>.

[47] For an overview of the German legislation see C Djeffal, 'La cybersécurité en Allemagne' *Revue de droit allemande* (2017) at <http://www.droit-allemand.org/>. See also H Leisterer, *Internetsicherheit in Europa: Zur Gewährleistung der Netz- und Informationssicherheit durch Informationsverwaltungsrecht* (Mohr Siebeck, Tübingen, 2017).

[48] For details, problems and limits see A Haase, *Bekämpfung der Computerkriminalität im Raum der Freiheit, der Sicherheit und des Rechts. Kompetenzen, Harmonisierungen und Kooperationsperspektiven*' (Mohr Siebeck, Tübingen, 2017).

the data subject. With a view to the possible damage for the data-subject or reliability of databases caused by manipulation or destruction of data the integrity of data is becoming a major concern also of cybersecurity and needs particular attention.

More is possible and necessary, however. Products are often put on the market without necessary checks to ensure their safe application and security.[49] Attackers abuse them for DDos attacks without the owners being aware of it. This cannot be accepted. Specific IT-related regulation on product safety and product liability needs to be adopted. But users too are to be made liable for damages arising from negligent or improper use of devices that do not meet minimum safety requirements, or for failing to regularly update their system as required. Insurers will assess the risks and, accordingly, fix the amount of fees to be paid. Only at this point will the real cost of IT systems including cybersecurity become visible.

This regulation should go hand in hand with new legislation on technical requirements for IT products regarding cybersecurity (including certification – CE-label). With the competence the EU has for the internal market, consumer and data protection, the EU should – and indeed seems to intend to – take the necessary measures.[50]

Cyberspace and military defence

States have recognised cyberspace as a new dimension of military defence, apart from land troops, the air force and the navy. This adds to the notion of cyberwar as a war in the proper meaning of the term. Some states are already spending billions of dollars not only on cyber defence but also on offensive cyberwar technology. Is this necessary in order to understand threats better, as a basis for defining effective strategies of defence? As has already been stated, with regard to the problem of attribution, classical concepts of response, hack-back and deterrence are questionable. Many states are not advanced in cyber defence. Bannelier and Christakis state in their preparatory study that 'the technical capabilities of the digital giants and their economic strength are not commensurate with those of many States, especially the less technologically advanced ones'.[51]

[49] An attempt to counter this is section 13(7) TMG (the law on telemedia –Telemediengesetz – TMG) providing for the duty of the telemedia and, in particular internet providers, to take appropriate measures on cybersecurity in accordance with the best available technologies.

[50] See the report on a leaked document preparing for meeting of the EU Ministers of the Interior: 'Beschlusspapier der Innenministerkonferenz: Plan gegen Spionage im Kühlschrank' in *RP Online* (23 May 2017) <http://www.rp-online.de/politik/deutschland/innenminister-planen-it-guetesiegel-fuer-smart-home-geraete-aid-1.6838817>.

[51] Bannelier and Christakis (n 22) 10.

More importantly, the question of whether offensive capabilities really add to cybersecurity remains an open question. As a matter of reason and humanity, international agreements have been reached to ban chemical and biological weapons and to limit, at least, nuclear armaments. Accordingly, for the costs of a new arms race and the unforeseeable new risks of damages for the civilian population, cyberwar is not an option and should be banned, while taxpayers' money should be invested in strategies and technology of resilience that make cyber-attacks impossible or, at least, ineffective.

Cybersecurity intelligence

Could intelligence activities be part of such strategies? Tapping internet cables and nots worldwide or other activities may help, one day, to finding the origins of attacks, at least geographically. New German legislation passed in 2015 includes provisions for powers of the Foreign Intelligence Service (BND) to detect serious risks of international cyber-attack.[52] But the definition of these powers is vague and general; in addition, action on foreign territory is not excluded. But what country would accept, in the absence of a cooperation agreement, such intelligence action led by foreign services on its own national territory? The Snowden revelations are a warning. In the name of national security, the NSA destroyed trust on a global scale. A legal regime containing clear limitation, strict control and cooperation should replace unilateral national action. Common intelligence with close parliamentary oversight should be established for well-defined purposes, including cybersecurity, at the European level.[53] Similarly, as a matter of common concern, joining all efforts at cybersecurity intelligence is a matter to be considered at the transatlantic and even at the global level, with due regard, however, to effective privacy and data protection.

[52] See section (1) phrase 3 N° 8 of the G10-law (G10 Gesetz). See also section 6 of the Law on the Foreign Intelligence Service (BND-Gesetz), with regard to communications and information from foreign countries. For a critical analysis see T Wetzling, 'Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls' SNV Policy Brief (June 2017) at <https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf>.

[53] E Macron, 'Humboldt Speech' in Berlin on 10 January 2017 (<https://www.rewi.hu-berlin.de/de/lf/oe/whi/FCE/2017/rede-macron>): 'We must also create a common intelligence system, overcoming national reluctance, that enables an effective tracking of criminals and terrorists, and, in the longer run, a common police force against organised crime and terrorism. We must face together, without being naive, the actual threats of the virtual world, cyberterrorism as well as any type of cyberattack'.

The work of international organisations on cybersecurity

States are already cooperating on cybersecurity within the framework of international organisations. The most important of these organisations is, of course, the UN. The result of a Russian initiative in 1998 and established under resolutions of the UN General Assembly,[54] the Global Group of Experts on Cybersecurity (GGE) has, since 2004, been reporting to the UN Secretary General on issues of priority and national strategies for cybersecurity.[55] While these reports contain important observations on the risks and on recent developments, and confirm the full application of international law to cyberspace (2013), they remain too general in their conclusions and recommendations. As a result, the GGE has been harshly criticised for its poor 'real world impact', and it has been suggested that it should become more inclusive, 'involving more stakeholders and producing outcomes that really shape policy, reflecting the realities of the cyber game'.[56] Its work, nonetheless, can be understood as an important effort to implement UN General Assembly Resolution 64/211 recognising 'that a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented'.[57] The 2017 Report, promised to be adopted and published in September 2017, has not been accomplished. Too controversial seem to have been the views of the participating states on questions of self-defence, the possible abuse of rights where the problem of attribution persists, or the question of openness or sovereign control over the national information space, if all countries had been ready to find consensus. Perhaps it was too ambitious to envisage agreement on 'how international law applies to the use of information and communications

[54] Originally based on a Russian initiative, the UNGA Resolution 53/70 on 'Developments in the Field of Information and Telecommunications in the Context of International Security' at <http://undocs.org/A/RES/53/70>. See the latest UNGA Resolution 68/243 of 9 January 2013: Developments in the field of information and telecommunications in the context of international security, <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/243>.

[55] See the overview of national reports at <https://www.un.org/disarmament/topics/informationsecurity/>. The latest examples of GGE reports to the UN Secretary General are the Report of 22 July 2015 at <http://undocs.org/A/70/174> and the Report of 19 July 2016 at <http://undocs.org/A/71/172>.

[56] See B Valeriano and A Pytlak, 'Cyber Security and the Coming Failure of the UN's Group of Governmental Experts' in *Foreign Policy & Defense* (31 August 2016) at <https://niskanencenter.org/blog/cyber-security-coming-failure-uns-group-governmental-experts/>.

[57] Resolution 64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (21 December 2009) at <https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf>. Similarly already the UN General Assembly Resolution 58/199 at <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/58/199>.

technologies by states', as the GGE was tasked, or things like confidence- and capacity-building at the UN level.[58] Or the GGE, a group of experts from national governments, even at this high level, is simply not a body that can produce far-reaching political or legal commitments of the international community as needed for effective protection of cybersecurity.

Another important international organisation dealing with questions of cybersecurity is the International Telecommunications Union (ITU).[59] A fundamental role given to the ITU by WISIS and the ITU governors is 'to build confidence and security in the use of Information and Communication Technologies (ICTs)'. The ITU runs a Global Cybersecurity Index (GCI), which is a multi-stakeholder initiative monitoring the cybersecurity commitments of different countries. Already in 2007 it launched the Global Cybersecurity Agenda (GCA) establishing a 'framework for international cooperation aimed at enhancing confidence and security in the information society'. ITU is also active in standardisation, with valuable work such as setting up the 'Focus Group on Smart Sustainable Cities'. In 2015 this group produced a technical report of high quality on 'cybersecurity, data protection and cyber resilience in smart sustainable cities'.[60] Yet, binding regulation on the technology or the use of the internet and, in particular, related to cybersecurity is not among the powers of ITU.

International conventions

In contrast, an international agreement can have legally binding effect, at least upon the participating states that ratified it. Few conventions have been concluded at a regional or international level for the purposes of cybersecurity. A first important achievement was the Budapest Convention on Cyber Crime of November 2001. It entered into force on 1 July 2004 and requires the criminalisation of all kinds of computer- and internet-related offences for the, so far, 54 contracting parties.

Another prominent example is the African Union Convention on Cyber Security and Personal Data Protection, adopted in June 2014.[61]

[58] GA Res 70/237 of 23 December 2015, point 5. For a critical comment see E Korzak, UN GGE on Cybersecurity: The End of an Era? *The Diplomat* (31 July 2017) at <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/>.

[59] See <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx>.

[60] See ITU-T Telecommunication Standardisation Sector of ITU, Focus Group on Smart Sustainable Cities (2/2015), link to pdf file at <https://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx>.

[61] At <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.

This is a remarkable step towards coordinated action, combining privacy and security in one document and imposing effective action on the contracting parties, including, in Article 26, the establishment of a 'Culture of Cybersecurity'.[62] The role of governments is defined here to 'provide leadership for the development of the cyber security culture within its borders', although in Article 27 the Convention also addresses 'cybersecurity governance' under the leadership of the governments, the establishment of an institutional framework and international cooperation (Article 28).

The Microsoft initiative of a 'Digital Geneva Convention to protect Cyberspace', already mentioned, has not yet received sufficient attention. It is meant to prohibit cyber-attacks on critical infrastructures, or causing damage to the global economy or to cloud-based services, causing major global disruption. It bans hacking personal accounts or 'private data held by journalists and private citizens involved in electoral processes' and requires states to refrain from inserting or requiring 'backdoors in mass-market commercial technology products' etc.[63] The many issues covered here reflect general concerns of cybersecurity and should guide upcoming negotiations at the international level. In spite of strong lobbying of Brad Smith for this project also at the 2017 IGF in Geneva,[64] this initiative does not seem to have received sufficient support by the governments.

These are promising initiatives, although they fail, if in force, either to go far enough in terms of providing concrete substance or to cover, as is needed, the territories of all countries and so to being effective at the global level. The experience is, that negotiation and ratification procedures of international conventions are most time-consuming and often take many years. This is particularly true in sensitive areas like internet regulation and cybersecurity. Technical developments are many times quicker than what governments can negotiate. Finally, international agreements, once in force, often suffer from the reluctance of states to completely carry out their duties. Compliance procedures, as known from international

[62] Para 1(a) reads: 'Each State Party undertakes to promote the culture of cyber security among all stakeholders, namely, governments, enterprises and the civil society, which develop, own, manage, operationalize and use information systems and networks. The culture of cyber security should lay emphasis on security in the development of information systems and networks, and on the adoption of new ways of thinking and behaving when using information systems as well as during communication or transactions across networks.' In February 2018 10 of 54 contracting parties have signed the Convention, one ratification so far, see at <https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_1.pdf>.

[63] See the text referred to (n 37).

[64] See the report of 18 December 2017 by *DigitalWatch*, 'High-Level Thematic Session: Shaping our Future Digital Global' at <https://dig.watch/sessions/high-level-thematic-session-shaping-our-future-digital-global-governance>.

environmental protection regimes like the Montreal Protocol on Subtances that Deplete the Ozone Layer[65] or the Åarhus Convention,[66] are difficult to achieve and of limited effect.

In the absence of effective means of enforcement and judicial protection, thus, new additional methods are needed to ensure cybersecurity at all levels. Given the shared responsibility of individuals, business enterprises, and state governments, with their respective tools and powers, an inclusive multi-stakeholder model of cybersecurity governance should be considered as the way forward.

VI. A framework for global cybersecurity governance

As has been shown above, with regard to security threats and also the responsibilities and instruments for providing cybersecurity, at present there is neither one single system nor any systematic approach for resolving the (self-made) problems that are arising with the increasing dependence of our societies on a secure and functioning internet. The picture, instead, is one of great complexity and deep fragmentation, while the risks are increasing. After examining the international law and cooperation on cybersecurity, the study of Bannelier and Christakis lists the organisations and forums dealing with cybersecurity, reaching the conclusion that: 'The problem, however, is that the proliferation of these initiatives in very diverse fora does not necessarily reflect good governance of cybersecurity.'[67]

Governance, as has already been mentioned, means the coordination of behaviour in society by multiple actors and factors.[68] Today, there is nobody to govern or even to coordinate the system as a whole. Social scientists may discern mechanisms and processes of a certain regularity from which some kind of coordination appears to be emerging. Such studies are important, but not sufficient. They may reveal that, in fact, there is little coordination. As a constitutionalist, and with an eye on the obligations arising from the above-mentioned fundamental principle of security, I am looking at the normative side and the question of how to organise effective mechanisms and processes of coordination.

[65] See Article 8 of the Convention and the Decisions on non-compliance in Handbook for the Montreal Protocol at <http://www.efcc.eu/media/1079/2016-ods-montreal_protocol-handbook.pdf> 348–473.

[66] Article 15 of the Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters, and the Guide to the Åarhus Convention Compliance Committee, at <http://www.unece.org/fileadmin/DAM/env/pp/compliance/CC_Guidance/Guide_to_the_ACCC_for_CC56_clean.pdf>.

[67] Bannelier and Christakis (n 22) 82.

[68] See (n 23).

Regulation presupposes a regulator. We have regulators at the national and at the EU level, but nothing comparable exists in transatlantic relations, and even less so at the global level. Governance includes regulators and regulation, but it is not limited to them. Institutions, bodies and platforms that already exist may need to be supplemented by other mechanisms and processes of cybersecurity governance in order to overcome complexity and fragmentation. The question, therefore, is what are – or what could be – processes of governance that might produce globally binding rules making cybersecurity a reality. With regard to the legitimacy of such rules the task is to identify some elements of a constitution of global cybersecurity governance.

In order to approach this task, some lessons can be learned from the existing mechanisms of multi-stakeholder governance, the work of which is – and should be – organised in a close dialogue with expert groups, institutions and networks. As the internet now offers new conditions for transboundary discourses and will-formation at a global level, it seems possible to develop further the existing structures towards an emerging global constitutional framework for setting rules on cybersecurity.

Multi-stakeholder governance mechanisms

Cybersecurity governance can be understood as a specific sector of internet governance, insofar as the latter is handled by private and/or multi-stakeholder organisations or platforms, such as ICANN for domain administration, IETF or ISO for standardisation and, more generally, the IGF as an open and global platform for the discussion of the most salient issues of internet governance. One of these issues is cybersecurity. While, except for the functioning of the domain name system, ICANN does not seem to be a key player in cybersecurity matters, IETF, ISO and the IGF certainly are.

The IETF and the ISO are setting technical standards which, though not binding, are of key importance to the interoperability and functioning of the internet. For years now, explicit descriptions of effects on cybersecurity have been one of the requirements that RfC's (requests for comments, instruments published by IETF as standards) have to meet, and RfC's have had to indicate the measures they take to ensure that security is taken care of in the implementation of the proposed technical standards. While IETF specialises in technical protocols like TCP/IP, the work of the International Standards Organisation (ISO) has a broader scope. ISO has issued numerous standards for cybersecurity analysis, engineering and management. The question is how to make sure that a certain level of protection is respected by these standards, allowing them to be implemented on a global scale.

Though the IGF does not take decisions, the expertise and views expressed at its sessions may be relevant for the establishment of such minimum requirements as the first stage of a normative process for globally applicable standards. The IGF has existed since 2006, having been established by the UN Secretary General at the request of WSIS. Its mandate was renewed for another ten years in 2015.[69] The discussions at the IGF are open to all stakeholders present or participating online. Cybersecurity was the first subtheme of the IGF in 2015,[70] and it seems also to be a priority issue at the December 2017 meeting in Geneva.[71] The further work of IGF should focus on the minimum requirements for IT products and the ways in which these can be met and concretised by standardisation, following the model of the 'new approach' adopted years ago by the EU for internal market harmonisation.[72] The discussions held at IGF are an important source of mutual information on best practices and experiences, the IGF provides room for deliberation and opinion-building and so can constitute a useful basis for the next steps of a normative process, as described below.[73]

Expert groups, institutions and networks

The IGF, however, is not the only platform to take up and discuss the issues of cybersecurity. At the Munich Security Conference in February 2017 the 'Global Commission on the Stability of Cyberspace' was launched by the Dutch government together with the Hague Centre for Strategic Studies and the EastWest Institute.[74] It was announced as 'a global body formed to convene key global stakeholders to develop proposals for norms and policy initiatives to improve the stability and security of cyberspace'.

[69] See the IGF webpage at <http://www.intgovforum.org/multilingual/tags/about> and the background paper at <http://www.intgovforum.org/cms/2015/IGF.24.06.2015.pdf>.

[70] One of the best practice forums at IGF 2016, however, was on cybersecurity: see Chair St. Amour at the preparatory 2017 MAG meeting day 3, at <http://www.intgovforum.org/multilingual/content/igf-2017-first-open-consultations-and-mag-meeting-day-3>.

[71] See M Kummer in the preparatory consultations: 'cybersecurity, as we all know, has really been an issue that has come to the fore' at: <http://www.intgovforum.org/multilingual/content/igf-2017-first-open-consultations-and-mag-meeting-day-1>. See also Kummer's statements at the 2017 MAG meeting day 3 (n 70), where he said that 'cybersecurity is an issue which is high on the agenda and it was also highlighted in the GA resolution which extended the IGF's mandate, so it is definitely, I think, an issue that is of interest to the broader community'.

[72] See the EU website on New Approach Standardisation in the Internal Market, at <http://www.newapproach.org/>, and J Pelkmans, 'The New Approach to Technical Harmonization and Standardization' (1987) 25 *Journal of Common Market Studies* 249.

[73] See section III.

[74] See the announcement by HCSS: <http://hcss.nl/news/global-commission-stability-cyberspace>.

For some years now, the Dutch National Cyber Security Centre has been organising the 'International One Conferences' with experts on cybersecurity.[75] A 'Commonwealth CyberSecurity Forum '17' was held in London in March 2017.[76] These and other initiatives and discussions in academic circles are gradually creating an informal network of practitioners, politicians and scientists that provide expertise and inform politics bottom up through a global deliberative process.

Special attention is deserved by the *Tallinn Manual on the International Law applicable to Cyber Warfare* (2013). This is the result of the work of an expert group working under the auspices of NATO, with 'the unofficial input of many States and over 50 peer reviewers'. This manual provides us with a number of important definitions, rules and profound advice relating to cyber warfare.[77] It seems, therefore, to represent the state of the art on almost all relevant questions, including the definition of terms like 'armed attack' or 'threat to international peace', the concepts of sovereignty, state responsibility, attribution and human rights, and how to protect civilians in cyberwar contexts, as well as more concrete issues like at what point the UN Security Council would be called upon to take action in the event of a cyber-attack under Chapter VII of the Charter of the United Nations.[78] A second edition of the Tallinn Manual was issued in 2017, now also covering legal peacetime regimes.[79] These works are of great value for the legal assessment of state action and responsibilities, even if they do not set binding rules but simply contribute to clarification of the existing international law with regard to cyber issues.

The problem with these studies, however, is that they do not overcome the traditional war-logic but, instead, strive to adapt the patterns of war and the law of war to the digital constellation. This is important, but it may not achieve what is needed for cybersecurity.

[75] See <https://www.ncsc.nl/english/conference>.

[76] See <http://www.cto.int/events/upcoming-events/commonwealth-cybersecurity-forum-2017/>.

[77] MN Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (Cambridge University Press, Cambridge, 2013) at <https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf>.

[78] For some comments on this impressive document see I Pernice, 'Vom Völkerrecht des Netzes zur Verfassung des Internets: Privacy und Digitale Sicherheit im Zeichen eines schrittweise Paradigmenwechsels' in HIIG Discussion Paper Series No. 2017-02 at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959257> 14–21.

[79] See <http://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf>. According to the advertising of CUP, 'it addresses such topics as sovereignty, state responsibility, human rights, and the law of air, space, and the sea. *Tallinn Manual 2.0* identifies 154 'black letter' rules governing cyber operations and provides extensive commentary on each rule.' On the same questions see also Bannelier and Christakis (n 22) 49–54.

Emergence of a global framework for rules on cybersecurity

People, stakeholders and experts active in the diverse forums and platforms focusing on cybersecurity not only meet and network with each other regularly but also produce a vast amount of knowledge, experience and creative thinking. New ideas flow from one forum to another and eventually become more or less accepted principles and some sort of shared common sense. Stakeholders learn from it, and knowingly or not, integrate what they 'bring home' from such discussions into their respective work. This way, they may ultimately inform government action or even legislative proposals. Much of it, though, is left to coincidence.

There may be many ways to organise these deliberative processes more systematically, so as to achieve more coordinated and thus more effective results. To be sure, the process should be based upon, and controlled by, public deliberation in order to receive democratically rooted legitimacy: citizens of the states should be involved and understand themselves as global citizens taking responsibility and having the final say, while it should be for the UN Secretary General to take responsibility for setting up a framework of coordination. The process should be fully transparent and based upon a broad, open global discourse actually made possible by the internet.[80]

Based upon already existing structures and processes and, in particular, cybersecurity policies at national and regional levels, a new model of a complementary normative process will be developed for cybersecurity governance at the global level, which is (a) built upon internet-enabled open information and deliberation that will serve as (b) a fundament for the establishment of bodies to elaborate and adopt a set of principles on cybersecurity to be (c) further concretised and made legally binding by combined processes of standardisation and legislation, while (d) more general globally binding norms will have to be agreed in the form of international conventions with the UN bodies taking responsibility for the coordination and supervision of the processes aiming at the adoption of globally applicable rules, the application of which (e) special UN bodies would monitor and courts at all levels would have to give effect to in individual cases.

(a) Deliberation: The Internet Governance Forum. The IGF is, meanwhile, a well-established multi-stakeholder global platform for open discussion of central issues related to the internet and its proper functioning. Its work

[80] For the theoretical basis and an outline of the processes see Pernice (n 2) and I Pernice, 'E-Democracy, the Global Citizen, and Multilevel Constitutionalism' in C Prins *et al.* (eds), *Digital Democracy in a Globalised World* (Edward Elgar, Cheltenham, 2017) 27.

is coupled with similar national forums or, at the European level: EURODIG. One section of their work should be developed to deal with the special issue of cybersecurity at all levels, as required – and guided – by the constitutional principle of security. It should systematically consider and, eventually, recommend appropriate use of all the instruments mentioned above as being part of the cybersecurity toolbox. Awareness, expertise and creative ideas on appropriate measures for consideration may emerge from these discussions.

(b) Principles: The model of NETmundial. On this basis, and drawing from the lessons learned in these forums, special multi-stakeholder bodies should be established for articulating and concretising general principles for cybersecurity with minimum requirements for products and normative guidelines to be translated, at the next stage, into globally applicable standards and legislation. NETmundial or the civil-society-born initiative for a Charter of Digital Fundamental Rights of the European Union[81] could serve as a model for such bodies. Similarly, the leading tech and internet-related industries should convene with users and other civil society organisations to agree upon globally applicable codes of conduct to guide standardisation and legislative processes. If a broad consensus could be achieved within such forums on certain basic principles, guidelines and security requirements, this outcome should be subject to scrutiny by the IGF together with the general public, and revisited and further developed as necessary before they are finally adopted by the forum of origin for transmission to the standardisation or legislative bodies or organisations at national, supranational and international level.

(c) Standards and regulation: IETF, ISO and legislators. IETF and ISO have proved to be an excellent framework for setting technical standards as a basis for interoperability, and they should focus on privacy- and cybersecurity engineering even more. Specifically with regard to cybersecurity, a close interaction of private standard-setting and legislative processes should be established. As with the system proposed in the EU's 'new approach', which has already been mentioned,[82] this could lead to a burden-sharing between legislators on the one hand, who would be responsible for setting up, on the basis of the principles adopted by the bodies described, minimum security requirements for products and services, and standardisation bodies like IETF or ISO on the other, which would turn these requirements

[81] See <https://digitalcharta.eu/#content>.
[82] See section 4 (with n 72).

into technical norms to be met by products or terms of services before they are put on the markets.

As far as principles focusing on the behaviour of states and governments, a similar kind of standardisation could be initiated at the international level within the framework of the UN. Concrete rules could take the form of soft law giving effect to the right to security as granted under Article 9 (1) of the International Covenant on Civil and Political Rights. A Global Declaration on State Duties and Responsibilities for Cybersecurity could lay down such essential requirements for states in respect of a ban of cyber warfare, responsibilities for cyber-attacks from their territory, mutual information and support in the event of cyber-incidents, and the enforcement of rules applicable to industry and individuals.

(d) International conventions and supervision: What role for the UN? Based upon the principles and guidelines elaborated within the framework of IGF and a forum like NETmundial, and a Global Declaration as mentioned above, it seems possible to elaborate, as a next step in the normative process, international conventions on the concrete obligations of states regarding their own behaviour as well as the adoption of national strategies and legislation relating to the protection and enforcement of cybersecurity. The Budapest Convention gives a hint for where to go, but there is a need not only to establish rules on cybercrime that are applicable globally so to ensure law enforcement in all states irrespective of where the crimes are committed, but also for binding law on other aspects of cybersecurity.

Furthermore, as cybersecurity is an issue that may eventually have a bearing on national security and international peace, it is time to consider seriously what role the UN Security Council should take in this regard. At least some supervisory powers should be given to this body, though it should be for the UN Secretary General to coordinate law-making and supervision at this level.

(e) Monitoring and enforcement of rules and rights. Enforcement of the generally accepted rules on cybersecurity will have to be ensured by national authorities, perhaps under the supervision of UN bodies like the GGE, to be further developed into a special agency, organised as a multi-stakeholder body and acting as the key authority of a compliance mechanism as well as a political forum in charge of monitoring the effects of existing rules and elaborating proposals for revision. More importantly, courts at the national and international level will have to play an increasing role, as soon as the relevant cybersecurity law comes into effect and, in particular, individual rights emerge from well-organised governance processes wordwide.

Towards global (multilevel) constitutionalism

The present outline of a model framework for global cybersecurity regulation certainly does not represent what we commonly understand as a Constitution. Nevertheless, it is suggested here that a discussion on possible developments should be commenced from which a constitutional setting for democratically legitimate regulation at the global level could emerge. It is similar to the concept of 'transnational popular sovereignty' developed by Milton Mueller with a view to overcoming the 'mismatch between internet territory and political territory' already mentioned.[83] But the aim is not to 'detach information policy from the state today' and construct a global polity based upon 'net nationalism' with 'a people of the internet', as he sees the system of ICANN.[84] Nor is it to conceive a 'community formed in and around internet connectivity' displacing 'specific pieces of territorial states' authority over global communication' with the aim that 'national governments have no sovereignty over content and to gradually de-legitimize these efforts' (of blocking and filtering access to websites and applications).[85] In contrast, the aim is to provide people with an instrument for effective, democratically legitimate action on matters beyond the reach of individual states more generally. Internet governance and, more particularly, cybersecurity governance, is only one issue. The term 'constitutional' is understood not to imply a state-like structure but an additional level of action through the establishment of institutions and processes that are rooted in the will of, and ultimately driven by, the citizens, defining themselves as global citizens with regard to such forums, bodies and institutions that are vested with specific powers for the achievement of objectives determined in the constituent texts through political processes in which they participate with the aim of setting globally applicable rules. Multilevel constitutionalism[86] is the normative theory that permits us to conceptualise such a constitutional framework, not as a centralised system of power at the global level, but as part of a composed constitutional system encompassing national,

[83] Mueller (n 9) 125–51.

[84] Ibid 130, 131–7.

[85] Ibid 142, 144–5, inspired by Perry Barlow's *Declaration of Independence of Cyberspace* (ibid 149).

[86] For the concept originally: I Pernice, 'Constitutional Law Implications for a State Participating in a Process of Regional Integration. German Constitution and "Multilevel Constitutionalism"' in E Riedel (ed), *German Reports on Public Law Presented to the XV International Congress on Comparative Law* (Nomos, Baden-Baden, 1998) 40.

supranational and global elements, so as to reflect the shared responsibilities of citizens and actors at the diverse levels.[87]

Global rule generation as one part of governance, and of global cybersecurity governance in particular, as an activity accepted by the global citizens as being democratically legitimate, would require inclusive processes of will formation and decision-making that do not replace but build upon national political and legislative processes, while adding a new, complementary level of action, control and judicial review. It would allow for the kinds of policies required by global challenges like cybersecurity and should be guided by globally agreed fundamental rights or principles like the principle of (cyber-)security. Accordingly, an emerging constitutional framework of cybersecurity governance would build upon existing national, supranational and international institutions and processes. It would be complementary to them and be limited to issues that are beyond the control of states.

Given the potential of the internet with regard to real-time information, education, deliberation and participation in political processes across borders, it is not impossible in the long run to imagine democratic decision-making at the global level on the concrete rights and duties not only of states but also of individuals and business enterprises. Such global decision-making could lead to the creation of regulations that are legally binding worldwide and may intervene where self-regulation and other forms of private ordering remain ineffective. E-democracy, in particular, is key to this development of global constitutionalism,[88] and it could, in future, supplement the existing toolbox of cybersecurity governance.

V. Conclusion

The digital revolution is posing new challenges that require responses that are beyond the reach of national policies. States alone are unable to ensure cybersecurity. Individuals, business, (tech) academia and public authorities share a common responsibility. And action is required at all levels: local, regional, national, supranational and global. Thus, in the 'digital constellation' effective cybersecurity governance includes all actors and all levels of action. It also requires a vision of regulation at global level, for which this article develops some elements along the lines of global (multilevel) constitutionalism.

[87] See I Pernice, 'The Global Dimension of Multilevel Constitutionalism: A Legal Response to the Challenges of Globalisation' in PM Dupuy *et al.* (eds), *Völkerrecht als Wertordnung/ Common Values in International Law: Festschrift für/Essays in Honour of Christian Tomuschat* (NP Engel, Arlington, VA, 2006) 973.

[88] For more details see Pernice (n 80) 37–44.

On the subject of constitutionalism and a legal framework for global cybersecurity governance, it should be stressed, first of all, that globally recognised human rights must be the foundation and a leading point of reference in the respective normative processes. Human dignity and personal freedoms, privacy and private property are just some of these rights. In particular, they include the protection of personal data and privacy. On the other hand, the constitutional right to security – or better: a fundamental principle of security[89] – is an incentive and guideline for action taken to effectively protect cybersecurity at all levels.

As a means of effectively containing cyber-risks, recourse to digital sovereignty is not the solution. The internet is global, and so must be the framework providing protection for its security and functioning. As – and as long as – the attribution of cyber-attacks and threats is technically impossible, deterrence and hack-back are not an option.

Instead, responsible risk assessment, of the kind that would be a precondition for any insurance scheme, as well as diligence in the selection and purchase of products and services, resilience through backups and the regular updating of all devices, are the first and foremost requirements to make cyberspace a safer place. But more is needed to achieve this objective: digital competence and specialised expertise in all disciplines is required – and must be developed further. Engineers and computer scientists, economists, social- communication and political scientists, even philosophers, psychologists and legal scientists are called upon to join in an interdisciplinary discourse on the best solutions in technology, as well as governance and regulatory processes. This is the way to progress in knowledge and to better inform the political processes.

The number of cyber-attacks is increasing, and so is awareness of the risks, and raising awareness of the shared responsibility of all actors for cybersecurity is becoming a priority. Furthermore, business, user organisations and general political processes should quickly focus on appropriate technical standards and certification on cybersecurity, while legislation is needed not only on information and alert systems but also on private responsibility and product liability and adequate insurance. Such normative processes should be undertaken at all levels, including the global level. For their democratic organisation at the global level, establishing a constitutional framework of global cybersecurity governance, the internet itself can play a crucial role.

[89] With regard to Article 6 of the European Charter of Fundamental Rights and Article 6 of the ECHR see Leuschner, *Vom Grundrecht zum Grundsatz* (n 46).