SWP Research Paper
Stiftung Wissenschaft und Politik
German Institute for International
and Security Affairs

Annegret Bendiek

European Cyber Security Policy

RP 13
October 2012
Berlin

SWP Research Papers are
peer reviewed by senior
researchers and the execu-
tive board of the Institute.
They express exclusively
the personal views of the
author(s).

SWP
Stiftung Wissenschaft
und Politik
German Institute
for International
and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Germany
Phone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1863-1053

Translation by
Tuomas Iso-Markku

(English version of
SWP-Studie 15/2012)

Table of Contents

5 **Problems and Recommendations**

7 **Challenges Facing the Market and the State**
8 Offenses against Private Property
10 Challenges to National Security

12 **The Multi-Level and Multi-Stakeholder Structure of Cyber Security Policy**
12 National Level
14 International Level
14 *International Organisations*
16 *Regional International Organisations*
17 *Transnational Forums*

19 **Cyber Security Policy in the European Union**
20 The Blurring of Boundaries between Internal and External Policy
21 Securitisation
22 Privatisation of Governance

24 **Guidelines for European Cyber Security Policy**
24 Summary
24 Recommendations

27 **Abbreviations**

Dr. Annegret Bendiek is a Senior Associate and deputy head of SWP's EU External Relations Division

European Cyber Security Policy

European security policy is changing in fundamental ways. The old threat scenario involving tank divisions from the East has been replaced by the challenge posed by invisible adversaries whose geographical source can often not be determined. Virtual attacks threatening critical infrastructure, government institutions and personal data form one of the key challenges to security policy in the 21st century. A secure Internet is essential to the protection of individual liberties, the right to informational self-determination and democracy as a whole.

The gradually developing European cyber security policy tries to establish minimum standards in all EU member states with regard to prevention, resilience and international cooperation. It aims to foster national security without compromising democratic principles or unduly violating individual liberties. However, it is hard to find a balance between these goals, and the EU's measures thus inevitably raise questions about the democratic implications of European cyber security policy: are the institutional structures and instruments of European cyber security policy compatible with the criteria of democratic governance? In order to answer this question, this study first outlines the main challenges related to the promotion of Internet security. After that, the study presents the institutional architecture of global cyber security policy and identifies the key principles of organisation behind European cyber security policy. In conclusion, the study assesses how compatible the institutional framework of European cyber security policy is with democratic criteria and discusses ways to enhance cyber security without endangering democratic principles. The study does not deal with the military or the legal dimension of data protection, technical aspects of internet regulation or the domestic political discourses in EU member states.

It is worthwhile to take a closer look at the EU, because the Union forms something of an institutional laboratory. What is tried out in the Union today could well be implemented at the international level in the future. Like the EU's counter-terrorism strategy before it, the Union's nascent cyber security strategy could thus become a focal point of international regulation and an important instrument for inner-Euro-

pean coordination. In other words, the EU's policies represent a model for the future of global regulation.

European cyber security policy is closely linked to both international and national regulatory processes. Put differently, European cyber security policy is formulated and implemented in a global multi-level, multi-stakeholder structure. This poses three central problems for democratic governance:

The blurring of the boundaries between internal and external policies: In the area of cyber security, it is almost impossible to maintain the traditional division into internal and external policies. Internet-based attacks can originate in Ghana, Russia or right next door, and it is often difficult (if not impossible) to identify the source of the attack. As a result, the boundaries between justice and home affairs policy on the one hand and foreign policy on the other become increasingly blurred. Threats can no longer be clearly defined as belonging to the area of responsibility of either policy field. A visible sign of this development is the increasing level of cooperation between authorities and institutions responsible for different policy fields. This erosion of traditional roles is more problematic in the EU than it is in the national context, but it is by no means a new phenomenon. In the last years, the development of European security policy has largely been driven by an internationalisation of the EU's justice and home affairs policy, whereas the role of the CFSP in cyber security policy is limited to the actions of the five dominant member states (Germany, France, Great Britain, the Netherlands and Sweden). In this new political structure, both the European Commission and the European Parliament gain new possibilities for influencing the policy-making process.

Securitisation: The EU used to have the goal to create a common "area of freedom, security and justice". However, at the face of new threats, the Commission and the member states tend to emphasize security over freedom, stressing the importance of introducing new security policy measures. In addition, private security companies have gained more and more influence in this policy field.

Privatisation of governance: Also the traditional distinction between the private sector and the public sector is increasingly fading in the emerging political structure. Without the technological expertise of private companies, it is difficult to identify the relevant threats and respond to them accordingly. Many private companies are also responsible for critical infrastructure in energy, health or transportation. Involving these companies in risk and crisis management as well as threat identification processes is a decisive part of maintaining public safety, which, on the other hand, has to be guaranteed by the institutions that have a constitutional mandate to do so.

To ensure the compatibility of the institutional structure and instruments of European cyber security policy with the principles of democratic governance, the following guidelines can be formulated: "Good governance" in European cyber security policy should meet such criteria as transparency, rule of law, accountability and participation. The constructive role of national parliaments in the institutional and material regulation of European cyber security policy is of particular importance, as parliaments are responsible for the communication with the general public. In democratic structures, parliaments should be the place where the relationship between security and freedom is being defined – especially when it comes to cyber security policy.

The negotiations over the International Convention on the Anti-Counterfeiting Trade Agreement (ACTA) made it clear that exclusive, opaque politics will lead to no results. Non-governmental groups such as representatives of the Internet industry, the civil society or the technical community should be included in political decision-making processes. This way, European coordination would follow the established principles of the internet culture: it would be "open", not "closed", "bottom up" instead of "top down" and "inclusive", not "exclusive".

Challenges Facing the Market and the State

One of the central problems for cyber security policy is that in the EU there exists no systematic, quantitative scheme to detect and disseminate information about cyber security threats.[1] Neither national nor international institutions have the technical capabilities or the legal competences required to register all Internet-based attacks on businesses, government agencies and private accounts.[2] Any assessment of the nature and degree of cyber risk will thus largely have to rely on expert analysis and government reports.[3]

These reports commonly divide cyber security threats into three categories: cybercrime, cyber espionage and cyber war.[4] The international community has so far failed to reach a consensus on a definition of these three concepts. However, cybercrime can be defined roughly as involving offences against property rights of non-state actors (e.g. phishing),[5] whereas cyber espionage stands for breaches in the databases of governmental or non-state enterprises by foreign government agencies. The term cyber war covers attempts of a state to harm another state by attacking it via the Internet. However, all of these working definitions remain ambiguous.[6] There are, furthermore, no clearly defined political or legal boundaries for differentiating between cybercrime, cyber espionage and cyber war, which makes classification all the more difficult.[7]

The lack of international consensus on definitions of cyber offences is not the result of disputes over technical and legal subtleties, but reflects a fundamental disagreement regarding the appropriateness and proper scope of government regulation in this policy field.[8] While some support the idea of establishing a

1 For more information on building cyber security scenarios, see Tessier Stall, *The Future of Cybersecurity*, Den Haag: The Hague Centre for Strategic Studies and TNO, 2011. For an overview of the system of cyberspace, see Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends* (Tel Aviv: Institute for National Security Studies, May 2012).

2 The action plan implementing the Stockholm Programme calls for the establishment of an Observatory for the Prevention of Crime (OPC), but the OPC will not be operational until 2013. Cf. David Brown, "The Stockholm Solution? Papering over the Cracks within the Area of Freedom, Security and Justice", *European Security* 20, no. 4 (December 2011) 4: 481–503.

3 For recent reports, see Alexander Klimburg and Heli Tirmaa-Klaar, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, a study requested by the European Parliament, PE 433.828 (Brussels, April 2011), 54. See also Myriam Dunn Cavelty, "The Militarisation of Cyber Security as a Source of Global Tension", in *Strategic Trends 2012: Key Developments in Global Affairs*, ed. Daniel Möckli (Zurich: Center for Strategic Studies [CSS], ETH Zurich, 2012), 103–24.

4 In the literature, the following four categories are often used: "Cyberwar – Warfare in cyberspace. This includes warfare attacks against a nation's military – forcing critical communications channels to fail, for example – and attacks against the civilian population. Cyberterrorism – The use of cyberspace to commit terrorist acts. An example might be hacking into a computer system to cause a nuclear power plant to melt down, a dam to open, or two airplanes to collide. [...] Cybercrime – Crime in cyberspace. This includes much of what we've already experienced: theft of intellectual property, extortion based on the threat of DDOS attacks, fraud based on identity theft, and so on. Cybervandalism – The script kiddies who deface websites for fun are technically criminals, but I think of them more as vandals or hooligans". Bruce Schneier, *Schneier on Security* (Blog), http://www.schneier.com/blog/archives/2007/06/cyberwar.html (accessed on 22 March 2012).

5 Phishing refers to the fraudulent acquisition of (or the attempt to acquire) sensitive information such as passwords or credit card information using electronic communications, whereby perpetrators impersonate trusted persons.

6 For an overview of different definitions of cybercrime, see Neil Robinson et al., *Feasibility Study for a European Cybercrime Centre*, prepared by RAND Europe for the European Commission (Brussels, 2012), 17–55.

7 Cf. Alexander Klimburg, "Mobilising Cyber Power", *Survival* 53, no. 1 (February–March 2011): 41–60; Friedrich Wilhelm Kriesel and David Kriesel, "Cyberwar – relevant für Sicherheit und Gesellschaft? Eine Problemanalyse", *Zeitschrift für Außen- und Sicherheitspolitik* 5, no. 4 (2011): 205–16 (214).

8 According to Kleinwächter, "three layers play a role in Internet regulation: the transport layer, i.e. the telecommunications infrastructure, that is regulated by national telecommunications law as well as by international treaties negotiated in the framework of the ITU; the protocol layer – in the stricter sense, 'the Internet' with its codes, standards, IP addresses and domain name systems – that is regulated by non-governmental global institutions such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Corporation for Assigned Names and Numbers (ICANN) or the Regional Internet Registries (RIRs); the application layer – i.e. all web-based services from

centralised intergovernmental organisation for Internet oversight, others favour a decentralised, multi-stakeholder governance model based on equal partnership between government, private sector, civil society, and technical experts.[9] These fundamental differences of opinion have been clearly visible in the recent debate over the extradition and prosecution of Wikileaks founder Julian Assange, in the dispute over the International Agreement on Anti-Counterfeiting Trade Agreement (ACTA),[10] as well as in the on-going quarrels about data mining practices.

All three examples involve both inter-state and national debates about the limits of legitimate state intervention and the boundaries of individual rights. In the Wikileaks case, the US prosecutors defined the publication of stolen, classified government documents as a felony, which resulted in the forfeiture of Wikileaks' organisational address (.org). This action was followed shortly thereafter by similar bans in Switzerland and Sweden. Those critical of the US attempts to shut down the website argue that Wikileaks is a neutral medium of information dissemination and should as such not be punished regardless of who uses it or for what purposes it is used.[11]

While corporate-interest groups hold that ACTA is necessary to protect intellectual property, the grand majority of the Internet public – consisting of home users as well as Internet-freedom advocates – perceive government measures in this area as a threat to the freedom on the Internet.[12] In a similar encounter, attempts by the EU to impose a directive on data retention met with strong resistance in Germany. The Federal Constitutional Court rejected the German Federal Diet's (Bundestag) measures transposing the EU directive by arguing that these infringed the right to secrecy of telecommunications (for a more detailed discussion of this case, see the section "Securitisation").

Considering the lack of conceptual clarity, it makes little sense to use the terms crime, espionage and war. A more practicable solution is to draw a distinction between threats to national security on the one hand and threats to the functioning of the market economy as well as offenses against private property on the other.

Offenses against Private Property

The Internet enables a wide variety of criminal actions that aim at the appropriation of property.[13] Instruments such as identity theft, phishing, spam and malicious code have rendered large-scale fraud offenses increasingly commonplace.[14] Financial losses from

e-commerce to social networks, which are primarily regulated by national law and, furthermore, by constitutional law, including freedom of expression and protection of property and privacy". Wolfgang Kleinwächter, "Wie reguliert man den Cyberspace? Die Quadratur des Dreiecks", *Heise Online – Telepolis*, 29 May 2012, http://www.heise.de/tp/druck/mb/artikel/34/34742/1.html (accessed on 2 June 2012; quote translated by T. I.-M.).

9 Cf. Wolfgang Kleinwächter, "Kalter Krieg im Cyberspace oder konstruktiver Dialog? Ausblick auf die Internetpolitik 2012", *Heise Online – Telepolis*, 20 January 2012, http://www.heise.de/tp/druck/mb/artikel/36/36266/1.html (accessed on 17 March 2012).

10 For more information, see *The Anti-Counterfeiting Trade Agreement (ACTA): an Assessment*, a study requested by the European Parliament, PE 433.859 (Brussels, 2011).

11 Cf. Geert Lovink and Patrice Riemens, "Die Anarchie der Transparenz", *Frankfurter Rundschau*, 7 December 2010: 32; see also François Heisbourg, "Leaks and Lessons", *Survival* 53, no. 1 (February–March 2011): 207–16.

12 For an excellent overview of this debate, see "Acta-Exegese: Ist es nun das Ende des freien Internet oder nicht?", *Frankfurter Allgemeine Zeitung* (online version), 23 February 2012, http://www.faz.net/aktu ell/feuilleton/medien/acta-exegese-ist-es-nun-das-ende-des-freien-internet-oder-nicht-11660030.html (accessed on 23 February 2012).

13 According to the European Commission, cybercrime comprises all "criminal acts committed using electronic communications networks and information systems or against such networks and systems". European Commission, Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, *Towards a General Policy on the Fight against Cyber Crime*, COM (2007) 267 final (Brussels, 22 May 2007).

14 The European Commission categorises cyber threats as follows: "*exploitation purposes*, such as 'advanced persistent threats' for economic and political espionage purposes (e.g. GhostNet), identity theft, the recent attacks against the Emissions Trading System or against government IT systems; *disruption purposes*, such as Distributed Denial of Service attacks or spamming generated via botnets (e.g. the Conficker network of 7 million machines or the Spanish-based Mariposa network of 12.7 million machines), Stuxnet and cut-off of communication means; *destruction purposes*. This is a scenario that has not yet materialised but, given the increasing pervasiveness of ICT [information and communications technology, added by the author] in Critical Infrastructure (e.g. smart grids and water systems), it cannot be ruled out for the years to come." *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. Achievements and Next Steps: Towards Global Cybersecurity*, COM(2011) 163 final (31 March 2011): 3–4.

identity theft as well as from fraudulent criminal practices targeting online banking and credit cards are growing rapidly. According to the crime statistics of the German police, approximately 38,000 criminal cases of this kind were reported in 2008. In 2010, the number of cases had risen to 60,000 and the losses amounted to 60 million euro.[15]

In a recent study, IT security company McAfee reported that 36 per cent of the business leaders, scientists and policy makers surveyed by the company in 27 European countries considered defence against cyber-attacks on critical infrastructure (e.g. utilities, banks, insurance, transportation) as important as missile defence.[16] Furthermore, 43 per cent of the respondents reported that hackers had attempted to damage their organisation's critical infrastructure. In the previous year's study, only 37 per cent of the respondents reported having fallen victim to such attacks.[17] The so called "Cyber Security Risks Report" published by Hewlett-Packard's Digital Vaccine Laboratories (DVLabs) underscores this trend.[18] According to the report, the first half of 2011 saw over 65 per cent more attacks on web applications than the first half of the previous year. The complexity of the attacks is also increasing, thus eroding the confidence of the majority of surveyed executives in their own IT security systems. Less than 30 per cent of executives believe that their own IT systems are well protected from attack.

According to the European Commission, one million people become victims of Internet crime daily.[19] This number includes online fraud, spam and emails from scammers asking for account information. Illegal websites sell credit card details for as little as one euro per card, whereas fake credit cards are available for EUR 140 and stolen bank account data for only EUR 60. Each day, some 600,000 Facebook accounts are blocked to prevent hackers from gaining entry. In 2009 alone, it was calculated that more than 6.7 million computers were infected with bots.[20]

According to the Internet security company McAfee, companies from the US and Europe suffer each year an estimated $ 1 trillion in damages when lost business, worthless research and development as well as additional spending on cyber defence are all counted together. Furthermore, the experiences of Sony and Adidas illustrate that also the public image of companies is vulnerable to cyber-attack. In April 2011, anonymous perpetrators managed to gain access to the information of more than 100 million of Sony's online customers. When Adidas fell victim to a similar attack in 2011, it was forced to take its website offline in an effort to protect customer data.

The pervasiveness of the problem is underscored by the estimate that there are currently about 30,000 vulnerability analysts selling their expertise to concerned producers and global organised crime syndicates.[21] In recent years, the European internal market and particularly Germany have become popular targets for cybercrime. However, according to the German government[22] and leading German business representatives, many medium-sized companies are insufficiently aware of the risks that arise from cyber criminality and the unwanted outflow of critical expertise.[23] This lack of awareness contrasts strongly with the increasing importance of cyber security issues to all modern service economies and, thus, to all EU mem-

15 Cf. Federal Bureau of Criminal Investigation, *Cybercrime: Bundeslagebild 2010*, p. 6, http://www.bka.de/nn_193360/DE/Publikationen/Jahresberi chteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true (accessed on June 21, 2012); for a recent estimation, see "Cyber Criminals Steal Millions from EU Banks", *EUObserver*, 27 June 2012.

16 Cf. Brigid Grauman, *Cybersecurity: The Vexed Question of Global Rules* (Brussels: Security and Defence Agenda, February 2012).

17 Cf. Jens Koenen, "Das Wettrüsten für den Cyber-War ist in vollem Gange", *Handelsblatt*, 31 January 2012: 23.

18 Cf. *Secure Your Network. 2010 Full Year Top Cyber Security Risks Report*, ed. Hewlett-Packard DVLabs (March 2011).

19 The number is based on a press release of the European Commission, *An EU Cyber Crime Centre to Fight Online Criminals and E-consumers*, IP/12/317 (Brussels, 28 March 2012).

20 Cf. ibid. Bots or botnets (short for robot network) are networks of compromised computers that can be controlled remotely and used for conducting coordinated attacks.

21 Michael Spehr, "Angriff auf IT-Systeme: Das Spiel der Hacker", *Frankfurter Allgemeine Zeitung*, 11 May 2011.

22 Interview with the Federal Minister of Interior Hans-Peter Friedrich, "'Cyberangriffe werden weiter zunehmen'", *Handelsblatt,* 3 February 2012: 17.

23 "Within a few minutes, a single employee with access to relevant data could copy all the information stored by a company on a USB flash drive and pass it on. [...] [I]nformation is still disseminated above all by people [...]. 'A uniform corporate culture and clear ethical guidelines provide protection' [...]", says Daimler's Head of corporate security, Sabine Wiedemann. See "Daimler-Sicherheitschefin Sabine Wiedemann referiert über Wirtschafts- und Industriespionage beim Neujahrsempfang des CDU-Kreisverbandes Enzkreis/Pforzheim", *Website of Gunther Krichbaum, Member of the German Bundestag and the Christian Democratic Union*, http://www.gunther-krichbaum.de/nc/startseite/aktuell/artikel/daimler-sicherheitschefin-sabine-wiedemann-referiert-ueber-wirtschafts-und-industriespionage-beim-n.html (accessed on 30 March 2012, quote translated by T. I.-M.).

ber states. Modern service economies are characterised by complex and interconnected modes of production. As a result, they are highly dependent on both a safe, Internet-based communication infrastructure and an effective protection of intellectual property. Secure modes of communication are the prerequisite for organising the different production phases, for transferring knowledge and for structuring the production chain. A significant proportion of the public infrastructure and services are also connected to the Internet and thus highly vulnerable to cyber-attacks.[24]

Challenges to National Security

The Internet also bears a wide variety of risks to national security. Since 2005, both federal agencies and industrial firms have experienced an increase in the number of attacks involving spy trojans.[25] At the 2011 Munich Security Conference, then-German Minister of Interior Thomas de Maizière revealed that the German government network is attacked four to five times a day by foreign intelligence services.[26] The problem of cyber espionage is exasperated by the fact that a number of states use cyber-attacks as a means to gather information.[27] In all probability, also the German authorities use the Internet to systematically collect data from other states. According to FOCUS, the Federal Intelligence Service BND has infiltrated 90 computers in Afghanistan and in the Democratic Republic of the Congo.[28] In order to perform cyber espionage operations, governments increasingly cooperate with private hacker groups that are able to break into corporate databases and steal strategically important knowledge. Experts estimate that there are hundreds of millions of malicious programs and more than 100 organisations that participate in military, intelligence or cyber terrorist operations.[29]

All such actions are generally subsumed under the heading cyber war.[30] Broadly defined, cyber war refers to all state actions that make use of internet-based instruments and aim at damaging another state.[31] When asked whether we are in cyber war, former CIA director Michael Hayden said: "That depends on the definition. For sure there is a national power struggle on the Internet. But most of it is spying, not war."[32] Currently, cyber warfare is conducted using botnets and worms. One of the most prominent botnet attacks took place in 2007, as a large a number of infected computers simultaneously requested access to the Estonian government servers, overrunning the servers' capacities and making the network temporarily unavailable. In March 2009, a network of compromised computers attacked the computer systems of government and private organisations in over 100 countries, accessing sensitive and confidential documents.[33] Similar attacks have occurred also in Malta (in 2004) and in Georgia during the conflict between Georgia and Russia in 2008.

The best-known case of a state-on-state attack by means of information technology became public in July 2010, as a malicious program now known as Stuxnet was discovered. It was widely speculated that Israel and the US used the software in an effort to disrupt

24 For an overview of national policies that aim at protecting critical infrastructures, see Elgin M. Brunner and Manuel Suter, *International CIIP Handbook 2008/2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies* (Zurich: CSS, 2008).
25 See Deutscher Bundestag, *Kleine Anfrage der Abgeordneten Jan Korte u.a.: Auskunft über Einsatz staatlicher Schadprogramme zur Computerspionage ("Staatstrojaner")*, Drucksache 17/7104 (25 October 2011).
26 Cf. Paul-Anton Krüger, "Wettrüsten im virtuellen Raum", *Süddeutsche Zeitung*, 7 February 2011; Jens Koenen et al., "Der Verteidigungsfall im Netz. Computerviren in der Hand von Terroristen", *Handelsblatt*, 27 January 2012: 21.
27 For a lengthier discussion of this problem, see Klimburg, "Mobilising Cyber Power" (see note 7).
28 Hubert Gude, "Geheimdienst: Trojaner im Dienst", *Focus*, 23 March 2009.
29 Numbers presented by Peter W. Singer, "Schlachtfelder der Zukunft", *Süddeutsche Zeitung*, 4 February 2011.
30 The following authors explicitly use the term cyberwar: Richard A. Clarke and Robert K. Knake, *World Wide War. Angriff aus dem Internet* (Hamburg, 2011); Sandro Gaycken, *Cyberwar. Das Internet als Kriegsschauplatz* (München, 2010); Id., *Cyberwar. Das Wettrüsten hat längst begonnen. Vom digitalen Angriff zum realen Ausnahmezustand* (München, 2012).
31 See Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks* (Washington, D.C.: Atlantic Council of the United States, January 2012); for an introduction into the legal dimension of cyber security policy, see Eneken Tikk, "Ten Rules for Cyber Security", *Survival* 53, no. 3 (June–July 2011): 119–32; for the strategic debate, see Paul Cornish et al., *On Cyber Warfare*, Chatham House Report (London: The Royal Institute of International Affairs, 2010), 25–34.
32 Cited in Christian Wernicke, "Spionage ist kein Krieg. Der ehemalige CIA-Chef Hayden warnt vor Cyber-Attacken, aber auch vor Hysterie", in: *Süddeutsche Zeitung*, 23 September 2010: 7 (quote translated by T. I.-M.).
33 Cf. European Commission, *Commission to Boost Europe's Defences against Cyber-attacks*, IP/10/1239 (Brussels, 30 September 2010).

the Iranian nuclear program.[34] Complex, discerning and adaptive, the Stuxnet virus required not only technical expertise but also significant human and financial resources to develop. Stuxnet is unlikely to remain an isolated case. It is estimated that there are some 100 state-sponsored and non-governmental teams world-wide attempting to replicate Stuxnet in order to device similar infrastructure-attacking malware.[35] In May 2012, IT experts identified a new malware known as Flame, Flamer or Skywiper. This virus has most likely been utilised ever since August 2010, and was originally developed by a state. According to estimates, thousands of computers above all in the Middle East have been infected by the virus that causes no physical damage but is able to collect enormous amounts of sensitive data. Rumours suggesting that the virus was created in Israel have never been officially denied.[36] Sutxnet and Flame are textbook examples "of the Janus-faced nature of conducting research on security vulnerabilities"[37] and an impressive example of the new offensive capabilities that many states are seeking to acquire.

The US Cyber Command, a department responsible for the digital national defence, now has more than 90,000 employees and a budget of about $ 3 million, whereas the US Army boasts of its capacity to disrupt the electrical grid of any city in the world through cyber-attacks.[38] In case of an armed conflict, information warfare is destined to play a key role, as almost all military capabilities now rely in one way or another on information technology. As a result, conflicts between major powers are unlikely to be limited to operations on conventional battlefield. Sandro Gaycken underlines the significance of information technology for modern warfare by pointing out that "in a way, cyber warfare enables the return of war despite the impossibility of major conventional conflicts".[39]

34 Farwell and Rohozinski hint that they believe Israel and the US stand behind these attacks. Cf. James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival* 53, no. 1 (February–March 2011): 23–40; David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran", *New York Times*, 1 June 2012; cf. id., *The Inheritance. The World Obama Confronts and the Challenges to American Power* (New York: Random House, 2012; forthcoming).

35 Uwe Proll, "Nach A-Waffen die IT-Waffen. Stuxnet verändert die globale Sicherheitsarchitektur", *Behörden Spiegel* (November 2010): 1.

36 Cf. "Computerschädling Flame: Experten enttarnen neue Cyberwaffe", *Spiegel Online*, 28 May 2012; "Cyber-Attacke: Israel preist Spionage-Virus Flame", *Spiegel Online*, 29 May 2012.

37 Frank Rieger, "Stuxnet: Angriff ist besser als Verteidigung", *Frankfurter Allgemeine Zeitung*, 17 January 2011 (quote translated by T. I.-M.).

38 Cited in Proll, "Nach A-Waffen die IT-Waffen" (see note 35).

39 Interview with Sandro Gaycken, "Mit Cyber-Kriegen lassen sich geostrategische Ziele realisieren", *Zeit Online*, 8 February 2012 (quote translated by T. I.-M.).

The Multi-Level and Multi-Stakeholder Structure of Cyber Security Policy

Considering the cyber security challenges facing European economies and states, the question that inevitably arises is how to incorporate cyber security policy into the institutional structure of the EU. Currently, governance in the area of cyber security is characterised by a certain duality. As far as regulatory issues are concerned, the European approach is generally liberal, meaning that private actors are encouraged to participate in the process. However, when it comes to questions of national security, there is a clear emphasis on the role of the state. Another characteristic feature of European cyber security policy is the plurality of actors. This plurality reveals not only the dynamic nature of the challenge but also the lack of clearly delineated areas of responsibility and accountability among the different institutions. In practice, cyber security policy has thus resorted to the "multi-stakeholder" model, where any group with the relevant expertise (businesses) or the required political authority (states) may participate in the policy-shaping process. In order to formulate guidelines for regulating the Internet in a manner that is both effective and, above all, legitimate, it is indispensable to know more about the international, regional and national actors that participate in shaping European cyber security policy.

National Level

Although the Internet is a highly unbounded space, legal and security responsibilities remain within the jurisdiction of the nation-state. Only at the national level is it possible to define cyber offenses, initiate law enforcement operations and punish offenders.[40] It is also the national level that links European and international regulatory processes to the democratic discourse, as public debates take place within the nation-state. Last but not least, it is the nation-state that possesses the competences and means to guarantee national security. Against this background, it is understandable that delicate questions concerning issues such as electronic surveillance methods are discussed in the national context.

In recent years, all OECD states have intensified their efforts to improve the protection of state institutions and private enterprises from Internet-based attacks.[41] The United States plays a leading role here: the Obama Administration has declared cyber security a strategic priority for defence and homeland security policy. Such policy commitments are not without financial backing, either. According to some estimates, the US government will spend 30 billion dollars on cyber security issues over the next five years alone. There is also a public debate in the US, including legislative proposals in 2010 and 2011, about the development of a so called Internet "kill switch" that would entrust the President with the ability to shut down portions of the US internet in order to protect critical infrastructure. In Europe, such possibility has so far not been discussed. Due to the fact that the biggest European carrier networks (Deutsche Telekom, France Télécom, British Telecom und Telefónica) are integrated across national boundaries, establishing a similar "kill switch" would require close cooperation and coordination between several states.

China and Russia are often mentioned as states that either tolerate or even actively support cyber-attacks on foreign government agencies, businesses and critical infrastructure.[42] German Federal Minister of Interior Hans-Peter Friedrich claims that there is clear evidence "that many cyber-attacks can be traced to an IP address within the Chinese address space".[43] Even

40 For a comparison of national cyber security strategies, see Alexander Seger, *Cybercrime Strategies*, Discussion paper (Strasbourg: Council of Europe, 14 October 2011).

41 The US Government, for example, wants to introduce the new "Einstein 3" defence system. This system should assist in protecting infrastructures that are essential to the US economy and allow for the real-time detection of intrusion attempts. Cf. Ulrich Hottelet, "Digitale Aufrüstung", *Die Zeit*, 2 February 2012: 22.

42 See for example Richard Clarke, "China's Cyberassault on America", *The Wall Street Journal*, 15 June 2011; Mike McConnell, Michael Chertoff and William Lynn, "China's Cyber Thievery Is National Policy – and Must Be Challenged", *The Wall Street Journal*, 27 January 2012.

43 Cf. "Bundesinnenminister Friedrich zur Cybersicherheit: 'Es ist richtig, die Alarmglocken zu läuten'", *Stern*, 15 March 2012 (quote translated by T. I.-M.).

the German government itself has become target of attacks from China. The National Security Agency (NSA) of the United States also lists Chinese computers as a common origin for espionage on US businesses and government agencies. Russia is accused on similar grounds. By contrast, it seems that Islamic fundamentalism does not currently play a central role in relation to cybercrime.[44]

Recognising the increased threat, also Germany attempts to improve its cyber defence capabilities.[45] In 2010, the conference of the German Ministers of the Interior approved a strategy to combat cybercrime. The strategy aims at fostering information exchange between public agencies and private stakeholders, enhancing crime control and increasing the responsibility of software providers and developers. The strategy also emphasises the importance of enhancing the skills of private and professional users. Exercises like LÜKEX 2011 as well as Germany's participation in the US-initiated Cyber Storm exercise in 2010 or the Eurocybex 2010 represent concrete steps on this road. The coalition agreement between CDU, CSU and FDP also includes measures for improving cyber security. These include the expansion of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) that is to become a central cyber security agency. In addition, all governmental cyber security competences are to be put into the hands of the Federal Government Commissioner for Information Technology. Furthermore, in February 2011 the federal government adopted a national cyber security strategy that includes an important institutional innovation, the National Cyber Defense Center (Nationales Cyber-Abwehrzentrum, NCAZ). The NCAZ integrates the capabilities of several agencies such as the Federal Office for Information Security, the Federal Bureau of Criminal Investigation (Bundeskriminalamt), the Federal Intelligence Service (Bundesnachrichtendienst, BND), the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV), the Federal Office for Citizen Protection and Disaster Support (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK), the Federal Police, the Customs Investigation Bureau (Zollkriminalamt, ZKA) and the Federal Defence Forces (Bundeswehr). The Federal Defence Forces contribute above all by bringing in the experiences and expertise of their Strategy Reconnaissance Command and, particularly, the so called Computer Network Operations unit ("Gruppe Computer Netzwerk Operationen").[46] The Bundeswehr even confirms that it has an "initial capability" to attack "enemy networks".[47]

The NCAZ's capacity to guarantee the security of governmental institutions, critical infrastructure and private businesses is contingent upon the degree to which it is able to combine the expertise and resources of the participating institutions. Apart from focusing resources, the NCAZ must try to consolidate existing knowledge on cyber security issues and take care of the communication with other European and international bodies. With its meagre staff of ten officers, the NCAZ can, however, not be expected to identify threats and develop appropriate countermeasures independently.

The structures of the German cyber security policy are a good example of how the formerly sharp distinction between internal and external security as well as the areas of responsibility between different government departments become increasingly blurred in this complex policy field. Cyber security issues undermine both the traditional distinction between civil defence, military defence and law enforcement on the one hand and the traditionally strict separation between public authorities and private enterprise on the other. The blurring of the boundaries between the public and the private sector is particularly evident in the efforts to build so called Computer Emergency Response Teams (CERTs) that gather information about computer attacks, develop plans for dealing with them and establish defence measures.[48] In most cases, the

44 For a discussion of cyber-jihad, see Asiem El Difraoui, *jihad.de. Jihadistische Online-Propaganda: Empfehlungen für Gegenmaßnahmen in Deutschland*, SWP Research Paper 5/2012 (Berlin: Stiftung Wissenschaft und Politik, February 2012; availabe only in German), 22ff.

45 For more information on the implementation of German cyber security policy, see Klaus-Dieter Fritsche, *Cyber-Sicherheit. Die Sicherheitsstrategie der Bundesregierung*, Analysen und Argumente 89 (Sankt Augustin: Konrad-Adenauer-Stiftung, March 2011).

46 The technical and operative centre is be supported by a national cyber security council. Members of the council include representatives of the Federal Chancellery as well as state secretaries from the Federal Foreign Office, the Federal Ministry of the Interior, the Federal Ministry of Defence, the Federal Ministry of Economics and Technology, the Federal Ministry of Justice, the Federal Ministry of Finance and the German *Länder*. Depending on the purpose of the meeting, also business representatives may be invited to participate.

47 "Bundeswehr bereit für Cyberangriffe", *Zeit Online*, 5 June 2012.

48 For a more detailed discussion of the use of the multi-stakeholder approach in the security sector (also in the frame-

CERTs coordinate both public and private expertise and aim at involving all concerned parties in the process. Private firms that own and operate critical infrastructure (such as energy, transport, health etc.) are of particular significance, as the protection of their resources serves not only the stakeholders themselves but the society as a whole. Consequently, the state has a vested interest in ensuring that these companies discharge their security responsibilities.

International Level

Effective legislation in the realm of cyber security needs to transcend the boundaries of the nation-state. The latter does maintain an important role by guaranteeing national security and protecting private property, but its possibilities to act in the borderless world of the Internet are extremely limited. It is thus of utmost importance that different national regulations are harmonised at the international level. Cybercrimes can be committed from within a state where the relevant criminal law provisions or the legal basis for any form of prosecution are lacking (the problem of so called "safe-havens"). In many countries, breaking into foreign databases, for example, constitutes no offence as long as direct damage is not detectable. Given these complications, governments' possibilities to act remain unclear: for instance, in the event of an attack on public infrastructure, who should the German prosecuting authorities pursue when the attack appears to have originated in a state that does not consider such as attack to constitute a criminal offence?

The following overview lists important formal and informal governmental and non-governmental actors that deal with cyber security issues and operate at the international level. The overview makes clear how broad the range of the participating actors is and gives an account of their interests as well as of the strategies they use to protect private property and/or national security from cyber-attacks. A central role in the cyber security field has been played by the General Assembly of the United Nations, but also organisations such as the International Telecommunication Union (ITU), the Group of 20 (G20), the Group of 8 (G8), NATO, the Shanghai group and Interpol have given impetus. In addition, there is a wide variety of transnational forums, regional organisations and non-governmental actors that are involved in cyber security issues.

International Organisations

The United Nations discusses cyber security issues extensively and has passed a number of resolutions on the subject. The Economic and Social Council adopted the resolutions 56/121 "Combating the Criminal Misuse of Information Technology" (2002) and 57/239 "Creation of a Global Culture of Cybersecurity" (2003). Both aim first and foremost at combatting the aforementioned safe-haven problem. The report 64/422 "Globalization and Interdependence" (2009), on the other hand, invites all UN member states to review their respective national efforts to protect critical information infrastructures. A further central UN document was adopted by the Disarmament Committee, whose resolution 64/386 "Developments in the Field of Information and Telecommunication in the Context of International Security" (2009) led to the establishment of an expert group dealing with developments in the cyber security field. In its report, the group warned that states are increasingly developing cyber warfare capacities.[49] Last but not least, the 2010 UN Report on Cyber Security launched a broad debate on the application of established principles of international law to cyberspace.[50]

At the operational level, the ITU has established itself as a major player in recent years,[51] mainly by organising events such as the Internet Governance Forum (IGF), the World Conference on International Telecommunications (WCIT) and the World Summit on the Information Society (WSIS).[52] The WCIT is a purely intergovernmental conference and its main

work of CERTs), see Andreas Schmidt, "At the Boundaries of Peer Production: The Organization of Internet Security Production in the Cases of Estonia 2007 and Conficker", *Telecommunications Policy* 36, no. 6 (July 2012): 451–61; Michel J. G. Van Eeten et al., "The Governance of Cybersecurity: A Framework for Policy", *International Journal of Critical Infrastructures* 2, no. 4 (2006): 357–78.

49 UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201 (30 July 2010).

50 Jeffrey Carr, *Inside Cyber Warfare. Mapping the Cyber Underworld* (Sebastopol, CA, 2010), Chapter 3.

51 ITU, http://www.itu.int (accessed on 20 March 2012).

52 ITU, *World Conference on International Telecommunications (WCIT-12)*, http://www.itu.int/en/wcit-12/Pages/default.aspx (accessed on 20 March 2012). For an overview of the WSIS process, see Milton L. Mueller, *Networks and States. The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010).

task is to review the so called International Telecommunications Regulations (ITR), a binding global treaty on telecommunications that was originally negotiated in 1988.

The planned revision of the ITR is, however, a highly controversial issue. This controversy is symptomatic of the persistent conflict within the international community over how to balance the demands of national security on the one hand and individual rights and liberties on the other. On the one side, there are the states that want to set up legally binding rules for almost all aspects of the Internet. In 2011, the so called Shanghai group (composed of China, Russia, Tajikistan and Uzbekistan), for example, proposed that an intergovernmental Internet Code of Conduct should be drafted. This codex would set "norms and rules for the conduct of States in cyberspace". The United Nations resolution of December 2011 endorses this proposal and requests the Secretary-General "to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures with regard to information space".[53] The underlying idea is that the sovereignty of states – threatened by the Internet – should be strengthened, and that any interference in the internal affairs of a state via the Internet should be forbidden.

UN support for the Shanghai group's initiative has been met with little enthusiasm, particularly on the part of the US. The Shanghai Group's approach runs contrary to the decentralised multi-stakeholder model favoured by the US. For the United States, international treaties on cyber policy are too rigid, too state-centric and too weak to effectively deter asymmetric cyber threats. In addition, the US is aware of its technological supremacy in all aspects concerning the Internet and, consequently, has only a limited interest in global Internet regulation. Instead, the US relies simply on an intensified dialogue on international norms of behaviour, confidence-building measures and strong involvement of private actors, as outlined in the "International Cyber Security Strategy" of the Obama Administration.

53 UN General Assembly, *General Assembly, Gravely Concerned about Status of UN Disarmament Machinery, Especially in Conference on Disarmament, Invites States to Explore Options*, GA/11182 (New York, 2 December 2011; cited by Kleinwächter, "Kalter Krieg im Cyberspace" [see note 9]).

The US has, however, been more supportive of the Improvement Working Group that was founded in 2010 in a bid to support the development of the Internet Governance Forum (IGF). The IGF is founded on the multi-stakeholder approach, involving governments, private enterprises, technical experts and representatives of civil society. Again, the opinion-forming processes are, however, rather complicated. While some advocate binding decisions, others praise the virtues of free and non-binding discussions between different stakeholders. There is also no agreement on the future role of the IGF. Above all China and Russia are unwilling to reinforce the IGF, as this would strengthen the role of non-state actors in cyber policy.

The fundamentally different approach of the United States and Russia to the appropriate organisation of global cyber security policy is particularly apparent in the framework of the Organisation for Security and Co-Operation in Europe (OSCE).[54] While Russia favours the idea of a universal cyber convention that codifies reasonable standards of state behaviour, the US stresses the importance of national regulations.[55] Germany has adopted a mediating role. At the computer expo CeBIT, chancellor Merkel expressed her support for formulating a codex that would guide government actions in cyberspace and should be signed by as many states as possible. At this point, it remains unclear as to which one of the international organisations (G8, G20, Council of Europe, the EU, NATO, OSCE or the UN) would be the most suitable point of contact for developing such a codex. However, as far as the operational level is concerned, the German government considers the European Network and Information Security Agency (ENISA) to have a duty to take the matter further.

In the meantime, also Interpol has become involved in Internet regulation.[56] The organisation plans to set

54 See United States Mission to the OSCE, *Cyber Security Keynote Address by Dr. Deborah Schneider, U.S. Department of State*, FSC-PC.DEL/30/10 (9 June 2010), http://www.osce.org/fsc/68524 (accessed on 23 February 2012).

55 Cf. Franz-Stefan Gady and Greg Austin, *Russia, the United States, and Cyber Diplomacy. Opening the Doors* (New York: EastWest Institute, 2010); *Statement by Mr. S. Shestakov, Representative of the Russian Federation, at the Joint Meeting of the OSCE Forum for Security Co-operation and the OSCE Permanent Council*, FSC-PC.DEL/31/10 (10 June 2010), http://www.osce.org/fsc/68693 (accessed on 23 March 2012).

56 For a good overview of the different legal frameworks applied in the fight against cyber criminality, see Marco Gercke, *Understanding Cybercrime: a Guide for Developing Countries*, 2. edition (Geneva: ITU, March 2011); see also ITU

up a central research and investigation unit to combat cybercrime.[57] Planned to be based in Singapore and scheduled to become operational in 2014, the so called Interpol Global Complex for Innovation (IGCI) will have research, development and training facilities as well as advanced computer forensic laboratories. The IGCI's work will mainly focus on evaluating and developing open source software for law enforcement authorities. In addition, the centre will provide assistance to states currently without sufficient cybercrime-fighting capabilities.

Another international forum that has been able to agree on common cyber security measures is the G8. The organisation's actions include the establishment of a joint working group on cybercrime (the so called Lyon-Rome Group) as well as the development of an emergency communications and support network. The latter should enable effective communication in cases where there is electronic evidence of a cyber offence and an urgent need for cooperation between law enforcement authorities from different states.

Regional International Organisations

Due to fundamental differences of opinion on regulatory issues between participating states, global international organisations have been hampered by conflict and unable to achieve much progress in cyber policy. The achievements of regional international organisations thus exceed those of the UN by far. The Council of Europe's 2001 Convention on Cybercrime stands as probably the most important regional agreement in the field of cyber security to date. Ratified in 2004, the convention provides common definitions of the various types of cybercrime and forms the basis for closer judicial cooperation between member states of the Council and several non-European countries, notably the United States and Canada. Many countries have also ratified an Additional Protocol to the Convention on Cybercrime concerning the criminalisation of racist or xenophobic acts.[58] In addition, both the Council of Europe and the OECD have developed their own principles for a safer Internet.[59] Both organisations emphasise the universality and integrity of a safe and secure Internet and support the involvement of private actors in the formulation of new rules. They also stress the importance of maintaining the existing architecture of the Internet with open standards and decentralised management. Importantly, the Council of Europe is also considering whether to invite private actors to take part in the intergovernmental negotiation process.

In recent years, also NATO has worked to develop an effective cyber security policy.[60] In its new strategic concept, NATO not only sets itself the goal of improving its military capabilities to avert cyber-attacks, but also promises to provide its member states with voluntary security standards for the protection of critical infrastructure.[61] In June 2011, NATO published its Cyber Defence Policy that emphasises the importance of cyber security and institutionalises a formal structure for policy coordination. The newly established NATO Cyber Defence Management Authority (CDMA) has been assigned the responsibility for coordination and strategic decisions on cyber security issues, whereas the Emerging Security Challenges Division coordinates the political and strategic overview of NATO's cyber defence measures. Operational responsibilities fall to the Computer Incident Response Capability – Technical Centre (NCIRC TC), whereas the so called Cooperative Cyber Defence Centre of Excellence (CCD COE) acts as an interface between the alliance on the one hand and the scientific community and the general public on the other.

The capacity of the Council of Europe and NATO to agree on common definitions and measures results from the fact that the member states of both organisations have cooperated closely for years. It goes to show that in order to adopt binding international rules to

Global Cybersecurity Agenda (GCA) – High Level Experts Group (HLEG), *Global Strategic Report* (Geneva: ITU, 2008).

57 Interpol, *The INTERPOL Global Complex for Innovation*, http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation (accessed on February 23, 2012).

58 Council of Europe, *Cybercrime*, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (accessed on 20 March 2012).

59 Cf. OECD, *Communiqué on Principles for Internet Policy Making*, www.oecd.org/dataoecd/40/21/48289796.pdf, and Council of Europe, *Internet Governance Principles*, http://www.coe.int/t/dghl/standardsetting/media-dataprotection/conf-internet-freedom/Internet%20Governance%20Principles.pdf (accessed on 21 January 2012).

60 Nato, *NATO and Cyber Defence*, http://www.nato.int/cps/en/SID-E1098959-0D8780E1/natolive/topics_78170.htm? (accessed on 20 March 2012).

61 Cf. Nato, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*, November 19, 2010, http://www.nato.int/cps/en/natolive/official_texts_68580.htm (accessed on 20 March 2012).

regulate the Internet, it is necessary that the negotiating states trust each other and have similar views on the right balance between individual liberties, market economy and public authority. Within Europe and between Europe and the United States this is largely the case. By contrast, the relationship of the states from both sides of the Atlantic with states such as China and Russia is dominated by mistrust and mutual accusations. Against this background, it seems unlikely that the international community would be able to establish truly global rules concerning the Internet or contribute to an effective global cyber defence. Currently, a more probable scenario is the creation of two parallel cyberspaces with distinct regulatory standards. This development would greatly affect both freedom and security on the Internet.

Transnational Forums

The US and other Western states base their cyber strategies largely on the positive experiences they have had in recent years with transnational forums that allow also private actors to participate.[62] The Forum of Incident Response and Security Teams (FIRST) stands as a good example of the benefits of the multi-stakeholder approach. At FIRST conferences, governmental and non-governmental IT security experts exchange information and experiences concerning attacks and malware, while simultaneously building personal relationships and mutual trust. FIRST also accredits domestic and non-governmental CERTs, offering them valuable expertise. Currently, FIRST and the ITU are trying to coordinate their activities in order to ensure that private and public expert knowledge are combined in the most effective manner. Ideally, this could lead to a new form of public-private partnership that would unite political authority and private knowledge, thus paving the way for innovative transnational solutions.

The multi-stakeholder approach, favoured by the US and most Western states, not only brings together organisations and forums from the national, international, regional and transnational level, but also supports the idea that private actors themselves assume the responsibility for coordinating their expertise. Important private actors in the cyber security field include the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Corporation for Assigned Names and Numbers (ICANN), the International Cyber Security Protection Alliance (ICSPA) and the Financial Services – Information Sharing and Analysis Centre (FS-ISAC). All of these privately operated organisations contribute to coordinating protection measures against cyber-attacks, develop appropriate instruments for the private sector and provide expertise and support to governmental and intergovernmental institutions. The existence of these private organisations reflects the widespread perception in Europe and the US that governmental institutions alone cannot be expected to identify critical cyber challenges or to develop appropriate, timely responses. This view forms the basis for Western regulatory liberalism in questions concerning the Internet and clearly differentiates it from the state-centric regulatory approach favoured by Russia and China.

The oldest non-governmental platform in the field of technical development of the Internet is the IETF.[63] It was formed in 1986 and brings together many of the most influential software programmers in the history of the Internet. The IETF has neither a clearly defined membership nor a strict hierarchical structure, rejecting "kings, presidents and voting" and relying on "rough consensus and running codes".[64]

A similar, non-hierarchical method has guided the formulation of the so called RFCs (Request for Comment). The RFCs are memorandums on internet-related issues and have been published since the late 1960s. They are regularly adopted by the IETF as internet standards. For example, the work of the regional internet registries (RIR), the regional organisations that manage the allocation of IP addresses, is not regulated by an international treaty but by RFCs adopted and published by the IETF.[65] Another important private non-profit institution is the IEEE that boasts more than 350,000 members and deals primarily with issues of connectivity between different devices and the harmonisation of technical standards.

When it comes to the development of standards and the allocation of IP addresses, a particularly important role is played by ICANN. ICANN is a non-profit

62 For basic information on the participation of private actors, see *PPPs in der Sicherheitspolitik: Chancen und Grenzen*, CSS Analysen zur Sicherheitspolitik, 111 (Zurich: CSS, April 2012).

63 The Internet Engineering Task Force (IETF), http://www.ietf.org (accessed on March 22, 2012).

64 *The Tao of IETF*, sub-point 3, http://www.ietf.org/tao.html#anchor3 (accessed on 22 March 2012).

65 Cf. Kleinwächter, "Wie reguliert man den Cyberspace?" (see note 8).

public-benefit corporation that operates under the laws of the State of California.[66] Contractually, ICANN is a quasi-autonomous non-governmental organization (QANGO) and cooperates closely with the US Department of Commerce.[67] Consequently, the US Government enjoys significantly more influence within the organization than other participating governments. The privileged position of the US within ICANN draws widespread criticism from the international community. In 2011, India, Brazil and South Africa (the so called IBSA countries) thus called for the creation of a Committee for Internet-Related Policies, a new intergovernmental UN body that would supervise ICANN and other similar organisations and also act as an international court of justice for Internet-related matters.

A further non-profit association of private enterprises is the ICSPA that was founded in 2011.[68] What makes the ICSPA especially interesting is the fact that it provides national law enforcement agencies with expertise and even material resources, thus touching upon a core area of state sovereignty.[69] The founding members of the organisation include IT security specialists such as Trend Micro and McAfee, the financial services corporation Visa Europe and the major British online retailer Shop Direct. In addition, the organisation cooperates closely with the European Police Office.

Last years have also witnessed the establishment of several sector-specific cooperation forums in the cyber security field. The FS-ISAC was launched in the late 1990s in response to an order by the US President demanding more cooperation between the public and private sectors to help protect critical infrastructure.[70] The main function of the FS-ISAC is to gather information from the financial industry, security companies, federal and state government agencies, law enforcement authorities as well as other interested governmental and non-governmental actors in order to contribute to the development of effective defence measures against cyber-attacks.

This overview of governance structures in the cyber policy field shows that the role of democratic governance in global cyber security politics is limited to the application of the delegation principle. Parliaments still struggle to find their place in this policy area. Even in the framework of the European Union it is evident that developments such as the blurring of boundaries between different policy areas, the securitisation and the privatisation of security all challenge the traditional separation of powers and, thus, the core of democratic governance.

66 Internet Corporation for Assigned Names and Numbers (ICANN), *Bylaws for Internet Corporation for Assigned Names and Numbers. A California Nonprofit Public-Benefit Corporation*, www.icann.org/en/general/bylaws.htm (accessed on 15 January 2012).

67 See ICANN, http://www.icann.org (accessed on 15 January 2012).

68 See ICSPA, https://www.icspa.org (accessed on 15 January 2012).

69 "Cybercrime-Allianz ICSPA sagt Web-Kriminellen den Kampf an", *TecChannel*, 6 July 2011, http://www.tecchannel.de/sicherheit/news/2036365/cybercrime_allianz_sagt_web_gangstern_den_kampf_an (accessed on 15 January 2012).

70 Further details can be found on the web page of FS-ISAC, http://www.fsisac.com (accessed on 15 January 2012).

Cyber Security Policy in the European Union

The nascent institutional structure of global Internet regulation is very important in view of the EU's own regulation efforts. The Union and its member states take part in almost all of the above-mentioned institutions and use these as platforms to cooperate with one another as well as with other states. However, the Union is not only another actor within the global institutional landscape, but also constitutes a highly developed institutional structure of its own. As an institutional framework for formulating cross-border policies, the EU is something of a model for what takes place on a global scale: developments that we witness in the EU today can be seen as a precursor of developments at the international level. The internal dynamics of the EU can thus give interesting insight into the future perspectives of global Internet regulation. In fact, the dynamics of global cyber security policy are often identical to those in the EU.[71]

Cyber security is now high on the political agenda of the EU.[72] The EU Commissioners Cecilia Malmström and Neelie Kroes as well as the High Representative Catherine Ashton are currently working on an EU strategy on cyber security. At a transatlantic forum in Washington in the beginning of May, Malmström gave a short overview of the core areas covered by the strategy that remains, according to her, a "work in progress". As a cross-cutting theme of the strategy, Malmström mentioned finding the right balance between freedom and security in cyber space. Other, more specific aims of the strategy include enhancing the EU's resilience and response capability, building public-private partnerships and advancing international cooperation on cyber security issues, especially with strategic partners.[73]

Already in March 2010, the European Commission proposed an action plan for the implementation of a concerted strategy to combat cybercrime.[74] In its proposal, the Commission stated that cybercrime "is borderless by nature" and that the fight against cyber threats requires "effective, adequate cross-border provisions". These measures should include enhanced mutual assistance in law enforcement operations.[75] According to the Commission, "the objective of building a coherent and cooperative approach within the EU remains as important as ever", but "it needs to be embedded into a global coordination strategy reaching out to key partners, be they individual nations or relevant international organisations".[76] Therefore, the EU and its institutions have established contacts with almost all international organisations and also allow these to participate in the European legislative process

71 One example is the European Commission's proposal for a strategy on the protection of children on the Internet. Hamadoun Touré, the secretary-general of the ITU, picked up the idea and called for the introduction of an international code for protecting children online, praising it as a small step towards the establishment an "International Code of Conduct for Information Security". "New Strategy to Make Internet Safer for Children", *Bulletin Quotidien Europe*, no. 10606 (3 May 2012): 7; Monika Ermert, "ITU will globales Abkommen für Cybersecurity vorantreiben", *Heise Online*, 17 May 2012.

72 The presidency trio formed by Spain, Belgium and Hungary, for example, explicitly dealt with cyber security issues in the so called M.A.D.R.I.D. report, published in May 2010. Council of the European Union, *First Main Assessment and Description Report for Internal Debate*, M.A.D.R.I.D. Report (Brussels, 26 May 2010), http://register.consilium.europa.eu/pdf/en/10/st10/st10203.en10.pdf (accessed on 20 January 2012). After the report was published, EU Counter-terrorism Coordinator Gilles de Kerchove announced that he was going to develop "a comprehensive approach to address cyberterrorism, cybercrime, cyberattacks/-war and cybersecurity". Council of the European Union, *Note from EU Counter-Terrorism Coordinator to Council/European Council, Subject: EU Counter-Terrorism Strategy*, Discussion Paper, 9685/10 (Brussels, 10 May 2010).

73 Cecilia Malmström, *The European Response to the Rising Cyber Threat*, Transatlantic Cyber Conference Organised by the Center for Strategic and International Studies, the European Security Roundtable and SRA International, Speech/12/315 (Washington, D.C., 2 May 2012).

74 Council of the European Union, *Draft Council Conclusions on an Action Plan to Implement the Concerted Strategy to Combat Cybercrime* (Brussels, 25 March 2010), http://register.consilium.europa.eu/pdf/de/10/st05/st05957-re02.de10.pdf> (accessed on 15 January 2012).

75 An example is the so called TransAtlantic IPR Portal that was launched at the meeting of the Transatlantic Economic Council in December 2010. This portal seeks "to encourage small business (SMEs) to break into foreign markets and avoid risks in terms of the violation of their intellectual property rights (IPR)". See http://ec.europa.eu/enterprise/initiatives/ipr/index_en.htm (accessed on 25 March 2012).

76 *Communication from the Commission on Critical Information Infrastructure Protection* (see note 14).

as far as this is possible and appears advisable. Consequently, the EU's approach could best be described as a multi-stakeholder approach coupled with intensified regional cooperation and a strong international dimension.

Joint cyber security exercises serve as a good example of the international dimension of the EU's cyber security policy. Exercises involving EU member states and the United States now take place regularly. Already in 2010, France, Germany, Hungary, Italy, the Netherlands, Sweden and the United Kingdom participated in "Cyber Storm", a civil-military cyber exercise sponsored by the US Department of Homeland Security. Also Australia, Canada, Japan and New Zealand as well as 60 private enterprises took part in the exercise. In November 2010, the so called High-Level EU-US Working Group on Cybersecurity and Cybercrime[77] was established and tasked with drafting "a cooperation programme culminating in a joint EU-US cyber-incident exercise by the end of 2011".[78] In the framework of the ensuing Cyber Atlantic exercise in 2011, experts from more than 20 countries simulated cyber-attacks on critical infrastructure such as power plants in order to test how cyber security cooperation between different states works.

The Blurring of Boundaries between Internal and External Policy

In a globalised world, it is no longer possible to clearly distinguish between an internal and an external space. This trend is evident also in the context of the EU: the formerly sharp distinction between internal and external policies is eroding, especially in the field of cyber security. European cyber security policy is largely the result of a close cooperation between institutions responsible for home and justice affairs policy as well as institutions responsible for foreign policy. This cooperation finds expression in the joint meetings of the Political and Security Committee (PSC) and the Committee on Operational Cooperation on Internal Security (COSI) as well as in the joint sessions of the Parliamentary Committee on Civil Liberties, Justice and Home Affairs (LIBE) and the Committee on Foreign Affairs (AFET).[79]

The meetings of these bodies have shown that it is very difficult to distinguish between internal and external security. For example, the protection of critical infrastructure (including energy, health, transport and communications) against cyber threats requires measures of both foreign policy and home and justice affairs policy.

The Commission's Communication on Critical Information Infrastructure Protection from March 2011[80] warns about the threat posed by cyber terrorism and cyber war and calls for more effective internal defence measures against these external threats. The Council document 10299/11, on the other hand, urges the member states to promote a new culture of risk analysis and management. The development of "coordinated actions to prevent, detect, mitigate and react to all kinds of disruptions"[81] should be understood as a central challenge at the national, European and international level. In order to effectively respond to attacks from third states, the Council suggests that the European Network and Information Security Agency (ENISA) should be modernised and reinforced. In addition, coordination between the National Computer Emergency Response Teams (CERT) should be enhanced.[82] The need to create new CERTs and improve the existing ones is emphasised also in the European Commission's communication "The EU Internal Security Strategy in Action".[83] Other important steps listed by the Commission include the setting up of a European Information Sharing and Alert System (EISAS) to detect attacks on critical infrastructure, the development of national contingency plans in cooperation with ENISA and the organisation of regular emergency exercises.

77 *EU-U.S. Summit 20 November 2010, Lisbon – Joint Statement*, MEMO/10/597 (Brussels, 20 November 2010).
78 *Cyber Security: EU and US Strengthen Transatlantic Cooperation in Face of Mounting Global Cyber-security and Cyber-crime Threats*, MEMO/11/246 (Brussels, 14 April 2011).
79 See Cecilia Malmström, *The EU Internal Security Strategy – What Does It Mean for the United States?* Discussion Organised by the Center for Transatlantic Relations, Speech/10/739, (Washington, D.C., 8 December 2010).
80 *Communication from the Commission on Critical Information Infrastructure Protection* (see note 14).
81 Council of the European Union, *Critical Information Infrastructure Protection "Achievements and Next Steps: Towards Global Cyber Security" (CIIP) – Adoption of Council Conclusions*, 10299/11 (Brussels, 19 May 2011), 2.
82 European Network and Information Security Agency (ENISA), http://www.enisa.europa.eu/media/.
83 Cf. also Council of the European Union, *Draft Council Conclusions on the Development of the External Dimension of the European Programme for Critical Infrastructure Protection*, 10662/11 (Brussels, 27 May 2011).

Cyber Europe 2010[84] made it clear that the EU's capacity to react to cyber threats is compromised by the unclear distribution of competences within the Union as well as the lack of effective internal structures in the smaller member states.[85] This shows that internal problems can rapidly turn into external vulnerabilities. In other words, domestic politics are highly relevant to security policy. Insufficient domestic regulation has an immediate negative effect on the security of other states.

Securitisation

A further trend that is visible in the EU is the securitisation of the agenda of the home and justice affairs policy. The Union's stated aim is to create an "area of freedom, security and justice". In recent years, the Commission and the member states have, however, focused almost exclusively on the security dimension, underlining the importance of responding to emerging threats by introducing ever new security measures.[86] The European Council's Stockholm Programme, for example, called for the formulation of "a comprehensive Union internal security strategy",[87] a document that pays only limited attention to data protection concerns. Unsurprisingly, the Commission's response to the Stockholm Programme is also written in a similar vein. Instead of proposing measures to protect and promote civil liberties and individual rights, the communication mostly talks about security issues such as organized criminality, cyber criminality, terrorism, border protection and disaster response.[88] Although the Commission notes in its communication that the EU's cyber security policy must be "based on common values including the rule of law and respect for fundamental rights", this statement has little substantial effect on the actions the Commission proposes. The Commission elaborates on the diverse security challenges facing the EU, the Union's security policy goals as well as the security measures that need to be taken. At the same time, the communication neglects to propose measures for the protection of the fundamental informational rights of EU citizens against invasive government policies. None of the actions listed in the annex of the Commission's strategy addresses this issue.

In current political discourse, security thus appears to trump freedom, a development echoed by the European Data Protection Supervisor's recent criticism that "some of the actions that derive from the ISS objectives may increase the risks for individuals' privacy and data protection".[89]

It is also striking that administrative actors have a more and more central role in European security policy. In matters concerning the implementation of the EU Internal Security Strategy, EU agencies will have the same rights as the EP, the Commission, the Council and the member states.[90] The most important agencies in the field of cyber security are ENISA, Europol, the European Police College (CEPOL), the European Maritime Safety Agency (EMSA) and the European External Action Service (EEAS). At the end of March 2012, the European Commission proposed the establishment of a further agency, the European Cybercrime Centre.[91] According to the Commission's proposal, the centre should become part of Europol and act as the focal point of the EU's fight against

84 Cf. Deutscher Bundestag, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko u.a.: Cyber-Übungen der Europäischen Union, der USA und die deutsche Beteiligung*, Drucksache 17/7578 (2 November 2011).

85 *Communication from the Commission on Critical Information Infrastructure Protection* (see note 14).

86 Cf. Madalina Busuioc and Deirdre Curtin, *The EU Internal Security Strategy, The EU Policy Cycle and The Role of (AFSJ) Agencies: Promise, Perils and Pre-requisites*, a study requested by the European Parliament, PE453.185 (Brussels, 2011); *Communication from the Commission: A Strategy on the External Dimension of the Area of Freedom, Security and Justice*, COM(2005) 491 final (Brussels, 12 October 2005); Myriam Dunn Cavelty and Kristian Søby Kristensen, "Introduction", in *Securing "the Homeland". Critical Infrastructure, Risk, and (In)Security*, ed. Myriam Dunn Cavelty and Kristian Søby Kristensen (London: Routledge, 2008).

87 "The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens", *Official Journal of the European Union*, C 115 (4 May 2010): 1, 17.

88 Cf. *Communication from the Commission to the European Parliament and the Council: The EU Internal Security Strategy in Action: Five Steps towards a More Secure Europe*, COM(2010) 673 final (Brussels, 22 November 2010).

89 "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council – 'EU Internal Security Strategy in Action: Five Steps towards a More Secure Europe'", *Official Journal of the European Union*, C 101 (1 April 2011): 6, 9.

90 For more information, see Deirdre Curtin, *Executive Power of the European Union. Law, Practices, and the Living Constitution* (New York, 2009).

91 *Communication from the Commission to the Council and the European Parliament, Tackling Crime in Our Digital Age: Establishing a European Cybercrime Centre*, COM(2012) 140 final (Brussels, 28 March 2012).

cybercrime. The centre's main tasks would be to help member states and EU organs to develop their operational and analytical capacities for conducting cybercrime investigations and to enhance international cooperation. In addition, the Commission encourages the member states to set up centres of excellence. These centres should be built up in close cooperation with Europol, the European Police College and Eurojust, and cooperate closely with universities and the IT industry.[92]

The European Parliament, on the other hand, is visibly marginalised:[93] "Incredible as it may appear, the principle strategic documents adopted to date by the European Council, the Council and the Commission seem to ignore the existence of the European Parliament altogether. While such a thing would, to say the least, have been surprising prior to the entry into force of the Lisbon Treaty, it is nothing less than inexplicable one year afterwards."[94]

The above-described shift in EU legislation is apparent also in the limited range of the Union's data protection policies. The EU's lack of interest to deal with issues concerning individual freedoms means that the Union's data protection rules remain "a patchwork".[95] And when the EU does enact legislation, its actions tend to compromise basic individual rights rather than to strengthen them. Directive 2006/24 on data retention is a typical example.[96] It obliges all EU member states to record the telephone calls of their citizens in order to support criminal investigations. The idea is to be able to trace all phone calls and mobile phone calls made as well as all emails sent during the last six to 24 months. In addition, service providers have to retain the location data of calls made or messages sent from a mobile phone or a smart phone. The retention of IP addresses, on the other hand, should – together with other available data – allow investigators to identify Internet users. The data retention directive considerably limits the citizens' right to informational self-determination. Originally, it was meant to be transposed into national law by September 15, 2007. Accordingly, Germany delivered a list of agreed transposition measures to the European Commission in 2008. However, the implementation process was stopped by the Federal Constitutional Court in 2010. According to the Court, the laws to implement the directive infringed the fundamental right to secrecy of telecommunications. This difference of opinion could well lead to a conflict between the Commission and the Federal Constitutional Court in the future.

Privatisation of Governance

At the international level, private actors participate more and more actively in cyber security policy. The same trend is evident also in European cyber security policy. Udo Helmbrecht, the director of ENISA, recently called for a stronger involvement of private actors in the agency's operations, including security exercises, public-private partnerships for network resilience, economic analysis and risk assessment, as well as campaigns to inform medium-sized businesses and the general public about cyber threats: "All security actors will [...] have to be working more closely together and develop better and more coordinated strategies".[97] ENISA has also drafted a detailed guide to establishing public-private partnerships, the so called European Public-Private Partnership for Resilience (EP3R). It is based on mutual interest: the EU and member state governments want to profit from the expertise of private actors, whereas these turn to the Union in hope for more effective legislation and better protection from cyber espionage and cyber-attacks.

The EU also seeks closer cooperation with Internet service providers and non-governmental organisations

92 Cf. *The EU Internal Security Strategy in Action* (see note 88).

93 For a lengthier discussion of this topic, see Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, a study requested by the European Parliament, PE453.207 (Brussels, 2011).

94 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Working Document on the European Union's Internal security Strategy, Rapporteur: Rita Borsellino*, PE458.598v01-00 (Brussel, 2011), 4.

95 Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for EU-Internal Information Exchange*, dissertation (Luxembourg, 2011).

96 "Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of available electronic communications services or of public communications networks and amending Directive 2002/58/EC", *Official Journal of the European Union*, L 105 (13 April 2006).

97 Cf. ENISA, *EU Agency Analysis of "Stuxnet" Malware: A Paradigm Shift in Threats and Critical Information Infrastructure Protection*, Press release (7 October 2010), http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1 (quoted in Matthias Monroy, "EU fürchtet Angriffe auf Informationssysteme", *Heise Online – Telepolis*, 11 October 2010).

in order to combat illegal online content, such messages endorsing terrorist activities. The Union plans to establish common guidelines for reporting and deleting such content. The EU's own internet platform Contact Initiative against Cybercrime for Industry and Law Enforcement (CICILE) should serve as a communication channel for relevant stakeholders.[98] Europol has also intensified its cooperation with private actors, such as ICPSA.

The European Parliament also considers private actors to be of central importance. The members of the Committee on Civil Liberties, Justice and Home Affairs of the EP recently urged Internet service providers to put more effort into protecting their IT systems. The committee also threatened to sanction companies that fail to meet the required minimum standards. In addition, the MEPs proposed tougher penalties for attacks on IT systems and demanded that offenders have to be consequently punished throughout the EU. Last but not least, the committee wants to oblige companies to both take preventive measures and cooperate with the police in criminal investigations. All in all, both the cooperation between different authorities and the cooperation between the public and the private sector in cyber security issues is to be enhanced.[99]

98 See Council of the European Union, *Council Conclusions Concerning an Action Plan to Implement the Concerted Strategy to Combat Cybercrime*, 15569/08 (Brussels, 26 April 2010); Council of the European Union, *Draft Council Conclusions on an Action Plan to Implement the Concerted Strategy to Combat Cybercrime*, 5957/2/10 (Brussels, 25 March 2010), http://www.statewatch.org/news/2010/mar/eu-council-revised-cyber-crime-conlcusions-5957-rev2-10.pdf (accessed on 22 March 2012).

99 Monika Hohlmeier, *EU-Strafrecht: Cyber-Angriffe sind kein Kavaliersdelikt/Konsequente Strafen gegen Hacker-Attacken/Unternehmen müssen ihre IT-Systeme besser schützen/EP-Innenausschuss zu neuer EU-Richtlinie*, Press release, 27 March 2012, http://www.monika-hohlmeier.de/eu-strafrecht-cyber-angriffe-sind-kein-kavaliersdelikt-konsequente-strafen-gegen-hacker-attacken-unternehmen-muessen-ihre-it-systeme-besser-schuetzen-ep-innenausschuss-zu-neuer-eu-richtlinie/ (accessed on 8 April 2012); see also Council of the European Union, *Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, Replacing Council Framework Decision 2005/222/JHA*, 10751/11 (Brussels, 30 May 2011).

Guidelines for European Cyber Security Policy

Taken together, the afore-presented developments suggest that the institutional structure of cyber security policy considerably deviates from the standards of democratic governance. Cyber security policy is being formulated at various political levels (national, European, international), is to a significant extent driven by private actors and defies any clear categorisation into internal or external policy. All three levels of cyber security policy are closely intertwined, forming a complex network-like structure (see the section "Summary" below). From the point of view of democratic governance, this multi-level structure is a source of several problems. These problems should be taken into account when proposals for new rules and regulations in this policy area are being formulated (see the section "Recommendations").

Summary

The institutional structure guiding global Internet regulation emerged spontaneously rather than as a result of constitutional considerations or a carefully crafted plan. This spontaneity is likely to remain a characteristic feature of global Internet politics also in the future. The political framework of global internet regulation builds on cooperation, coordination and co-optation, and no stakeholder alone is strong enough to change its operational logic. Neither the United States nor the EU (or any other international organisation) is in a position to unilaterally shape global cyber security policy.

European cyber security policy is formulated within a multi-level, multi-stakeholder structure. Within this political framework, consensus-building across different sectors and private expertise are of particular importance. For the first time, experts from private companies and organizations thus have the chance to take part in shaping security policy. In the past, private actors have only been involved in less sensitive policy areas, such as economic policy, environmental policy and utility policy. Although increasing private sector participation involves obvious risks, it can also be optimistically seen as a first step on the road towards a more democratic security policy.

EU agencies and transnational non-governmental organisations are the principal channels through which private actors can be integrated into the political process whenever their expertise is needed. In such cases, private actors are likely to be able to use their comparative technological advantage to decisively influence the political agenda of the EU. Private actors also profit from the fact that neither the Commission nor the Council has enough agenda-setting power or the capacity to shape the decision-making process as a whole. Instead, expertise and authority in this policy area are dispersed across different actors and layers, and coordination across various stakeholders is at least as important as building majorities. With the exception of cases in which the co-decision procedure applies, the European Parliament has only a very limited role in cyber security policy.

For the most part, decision-making in the cyber policy field is characterised by a lack of transparency and accountability. Actors with no special expertise or political authority are excluded from decision-making at national, European and international level. National parliaments, for example, only play a subordinated role at all three levels, being almost completely absent from the European level and hardly participating in the development of national cyber defence measures. Considering the importance of parliaments for democratic governance, this state of affairs constitutes a serious problem. At least at the national and European level, serious efforts are thus needed to provide national parliaments with the necessary means to both follow the development of European cyber security policy and to deliver well-founded opinions on cyber security issues. At the moment, both the Bundestag and the European Parliament lack the scientific expertise and resources to perform these functions.

Recommendations

How should the new European cyber security architecture be evaluated? And how is it possible to measure its democratic credentials? According to the European Commission's White Paper on European

governance,[100] democratic decision-making processes should be characterised by openness, rule of law, accountability and participation. In this vein, public-private partnerships are welcome additions to the legislative process if they combine social expertise and government authority in a meaningful way. Furthermore, it is important that so called diffuse interests (i.e. interest groups that are organised only loosely or not at all) as well as concerns related to the right of informational self-determination are taken into consideration in the process. Wider public participation should also be possible – Internet regulation is, after all, an issue that touches upon various aspects of political and economic life as well as upon the private sphere of citizens. The pervasiveness of the Internet and the ensuing consequences of Internet regulation for society as a whole should be more intensively discussed above all in the cyber security field.

In the current political discourse, it is possible to identify at least five concrete proposals for improving security in cyber space. These five proposals can be evaluated on the basis of the criteria discussed above.

Raising awareness of cyber threats: Almost all institutions and individuals dealing with questions of Internet security stress that it is indispensable to raise public and political awareness of the threats posed by cyber criminality and cyber terrorism. This requires a high degree of transparency concerning the different cyber threats. Representatives of law enforcement agencies must receive adequate training and be properly equipped in order to arrest and prosecute Internet criminals and terrorists. The Bundestag and various national ministries have already established committees in order to meet these challenges. Also national security services have taken important measures. However, as far as the above-mentioned transparency dimension is concerned, there is still plenty of room for improvement. A notable shortcoming is the lack of information exchange between the parliament and the government as well as between private companies and government security authorities concerning the quantity and quality of cyber-attacks.

Collecting more information on cyber threats: The EU and the US have both recently launched widely-debated initiatives to oblige private companies to report cyber-attacks to the national security authorities. The US Government defends the initiative as a necessary measure to guarantee national security. However, to its opponents the plan represents a violation of the right to informational self-determination, i.e. the right of each company to decide independently when it wants to release data and whom it wants to provide access to that data. As such, the debate underlines the difficulty of finding the right balance between such central values as security and freedom and shows, once again, how important it is to discuss issues of Internet regulation in an open, participatory process that involves parliamentary representation.

Enhancing prosecution of cybercrime cases: At some point, all discussions on cyber security issues tend to mention deterrence and debate the possibility of imposing tougher penalties for cyber offences. It is undisputed that a cyber-attack on critical infrastructure poses a serious threat to national security and launching such an attack should therefore lead to a severe punishment. There is also no doubt that breaking into a database is an offence that is comparable to breaking into a building. While the provisions of the German Criminal Code allow for the prosecution of such offences, international coordination on this issue is still insufficient. In order to avoid legal grey areas and to guarantee the rule of law also in cyber space, it is important to harmonise legal provisions on a global scale.

Revising the German War Weapons Control Act: A revision of the German War Weapons Act should be considered in order to extend its provisions to malware. Malware can be utilised for attacks against other states or their critical infrastructure and can cause similar damage as other war weapons. The export of such software should thus be controlled. The same goes for programs that are used by authoritarian states for surveillance or for disrupting communication between opposition forces. Companies should disclose information concerning the export of such programs.

Drafting a global code of conduct for cyberspace: In order to increase accountability, it is essential to draft a global code of conduct for the Internet. This codex should apply to both states and non-governmental actors such as companies or individuals and clearly define different types of cyber offences. These include attacking critical infrastructure, breaking into a database, accessing or utilising private data without authorisation, as well as using software for espionage. So far, the US has blocked all efforts to formulate such a codex. Especially states with limited resources find it hard to accept the US resistance. As long as there is no global code of conduct, the technologically most advanced

100 Cf. European Commission, *European Governance: A White Paper*, COM(2001) 428 final (Brussels, 25 July 2001).

state – the United States – is free to do what it wants in cyber space without having to face charges for its actions, whereas other states remain in a highly vulnerable position.

If all of the measures listed above fail to have the desired impact (or to find enough support to be implemented in the first place), this is likely to lead to calls for more a restricted Internet. In fact, the idea of limiting the reach of the Internet already has its supporters: while some argue simply that sensitive data should be kept off the Internet, others go as far as to demand that access to certain information should be denied altogether. At its most extreme, this strategy aims at complete isolation. Iran, for example, attempts to disconnect its national network from the global Internet in order to reduce the risk of cyber-attacks against its (nuclear) industry. The self-imposed isolation also serves to curb the free flow of information on the Internet and prevents the citizens from using the web for criticizing the government. Similar measures have been taken in China.

Creating a nationally self-sufficient Internet system is a delicate political instrument and bears serious risks for individual liberties. Against this background, it appears all the more important to make progress in the five issue areas outlined above.[101] In order for the proposed measures to work, it is indispensable to involve private actors. At the same time, regulative strategies such as the planned EU strategy on cyber security cannot be measured only by their efficiency. Instead, they also have to fulfil the fundamental criteria of democratic governance: transparency, rule of law, accountability and participation.

101 If states refuse to establish preventative norms, they put the entire Internet at risk. See Bruce Schneier, "Cyberwar Treaties", *Schneier on Security* (Blog), 14 June 2012, http://www.schneier.com/blog/archives/2012/06/cyberwar_treati.html?utm_medium=twitter&utm_source=twitterfeed (accessed on 26 June 2012).

Abbreviations

ACTA	Anti-Counterfeiting Trade Agreement
AFET	Committee on Foreign Affairs/ Commission des affaires étrangères (EP)
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe/Federal Office for Citizen Protection and Disaster Support
BfV	Bundesamt für Verfassungsschutz/Federal Office for the Protection of the Constitution
BND	Bundesnachrichtendienst/Federal Intelligence Service
BSI	Bundesamt für Sicherheit in der Informations-technik/Federal Office for Information Security
CCD COE	Cooperative Cyber Defence Centre of Excellence
CDMA	Cyber Defence Management Authority
CDU	Christlich Demokratische Union/Christian Democratic Union
CEPOL	European Police College
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIRP	Committee for Internet-Related Policies (UN)
COSI	Standing Committee on Operational Cooperation on Internal Security
CSU	Christlich-Soziale Union/Christian Social Union of Bavaria
EEAS	European External Action Service
EISAS	European Information Sharing and Alert System
EMSA	European Maritime Safety Agency
ENISA	European Network and Information Security Agency
EP	European Parliament
EP3R	European Public-Private Partnership for Resilience
EU	European Union
Eurojust	European Union's Judicial Cooperation Unit
Europol	European Police Office
FDP	Freie Demokratische Partei/Free Democratic Party
FIRST	Forum of Incident Response and Security Teams
FS-ISAC	Financial Services – Information Sharing and Analysis Center
G8	Group of Eight
G20	Group of Twenty
ICANN	Internet Corporation for Assigned Names and Numbers
ICSPA	International Cyber Security Protection Alliance
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGCI	Interpol Global Complex for Innovation
IGF	Internet Governance Forum
IP	Internet Protocol
IT	Information Technology
ITR	International Telecommunication Regulations
ITU	International Telecommunication Union
LIBE	Committee on Civil Liberties, Justice and Home Affairs (EP)
NATO	North Atlantic Treaty Organization
NCAZ	Nationales Cyber-Abwehrzentrum/National Cyber Defense Center
NCIRC TC	Nato Computer Incident Response Capability – Technical Centre
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OPC	Observatory for the Prevention of Crime
OSCE	Organisation for Security and Co-Operation in Europe
PSC	Political and Security Committee
QANGO	Quasi-autonomous Non-governmental Organization
RFC	Request for Comments
RiR	Regional Internet Registry
SMS	Short Message Service
UN	United Nations
US	United States of America
W3C	World Wide Web Consortium
WCIT	World Conference on International Telecommunications
WSIS	World Summit on the Information Society
ZKA	Zollkriminalamt/Customs Investigation Bureau