Bendiek, Annegret

Research Report

Tests of partnership: Transatlantic cooperation in cyber security, internet governance, and data protection

SWP Research Paper, No. RP 5/2014

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Bendiek, Annegret (2014) : Tests of partnership: Transatlantic cooperation in cyber security, internet governance, and data protection, SWP Research Paper, No. RP 5/2014, Stiftung Wissenschaft und Politik (SWP), Berlin

This Version is available at:
https://hdl.handle.net/10419/253145

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

Annegret Bendiek

Tests of Partnership

Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection

RP 5
March 2014
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 Scott Stock
Gissendanner

(English version of
SWP-Studie 26/2013)

The translation of the initial
German release of this paper
was made possible through
the generous support of the
Transatlantic Academy and
the German Marshall Fund of
the United States.

This English version has also
been published by the
Transatlantic Academy,
http://www.gmfus.org/
archives/tests-of-partnership-
transatlantic-cooperation-in-
cyber-security-internet-
governance-and-data-
protection/

Table of Contents

Dr. Annegret Bendiek is a Senior Associate and Deputy Head of SWP's EU External Relations Division and currently Robert Bosch Public Fellow at the Transatlantic Academy in Washington

Tests of Partnership.
Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection

Edward Snowden's revelations of the scope of surveillance conducted by U.S. intelligence agencies have been the subject of much debate in Europe, especially in Germany. It came as a surprise to many that Europe's closest political ally has been intercepting private communications on a large scale, even going so far as to wiretap high-ranking officials of the European Union and its member states. Moreover, the U.S. government has been and continues to use the most important Internet platforms in daily use by Europeans — Google, Yahoo, Amazon, and others —to acquire information about European citizens, through methods that are fundamentally opposed to European legal sensibilities and to the fundamental right of informational self-determination. These practices have damaged the transatlantic partnership between Europe and the United States and may well have resulted in a breach of trust that will prove irreparable. Some observers argue that the two partners' differences over the right balance between cyber security and data protection are ultimately irreconcilable because they are the product of differing geostrategic positions. Because U.S. engagement is more global in scope, the threats to U.S. security are thought to be more serious than those faced by Europe. For this reason, "Venus Europe" and "Mars America" are unlikely to find common ground on cyber security policy and data protection in the near future. Indeed, the kinds of cooperation in global multistakeholder Internet governance that have been taken for granted in the past may well become increasingly controversial in the future.

Although relations are currently being tested, the transatlantic cyber partnership continues to stand on a solid normative and institutional foundation. Both sides agree on the fundamentals of Internet regulation. Both are of the conviction that universal accessibility to the Internet is extraordinarily useful not only for democratic decision-making and free markets but also for the future of the liberal democratic order. And both sides are united also in the search for effective means to limit malicious software, to fight crime, and to secure critical infrastructure.

The controversy surrounding the NSA's espionage activities exposed differences in what the United States and EU member countries consider to be the legitimate means and methods of reaching their common goals. It also revealed that they have different approaches to handling normative dissonance. Nevertheless, it certainly should not be misunderstood as an existential threat to the transatlantic partnership. Instead, transatlantic differences can and should be speedily resolved through political dialogue. Three major problem areas must be dealt with in this process.

Global: The present mode of Internet regulation lopsidedly favors the United States and does not sufficiently integrate the emerging powers of Brazil, India, South Africa, China, and Russia. The concept of "multistakeholder governance" may rhetorically evoke egalitarian fairness, but in practice camouflages the fact that U.S. interests and U.S. corporations are de facto the most important agenda setters in Internet governance. Financially weaker actors wield precious little influence in central institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) or the Internet Governance Forum (IGF). The United States and Europe have defended in unison the existing governance model for a long time. The recent disclosures about U.S. surveillance practices, however, are causing more Europeans to question the status quo, and a realignment with states like Brazil is taking place.

Transatlantic: The EU and the United States diverge sharply in their views on the most important goals for transatlantic cooperation between national governments in the field of cyber security policy, especially regarding the appropriate balance of security and freedom. U.S. cyberspace policy is driven increasingly by the military logic of deterrence, which entails maintaining and strengthening an offensive capacity. Europeans, however, treat the security aspects of cyberspace policy as a police matter, and their main goal is strengthening systemic resilience and resistance to attack and fraud. Accordingly, U.S. and European intelligence agencies differ in their areas of responsibility and authority, and they have acquired quite different attitudes regarding informational self-determination and other civil liberties. To prevent these differences from degenerating into massive conflict, both sides must engage each other more openly. Success depends on the United States and Europe recognizing that on both sides, domestic politics limit the range of feasible compromise. As long as the United States seeks to maintain its position as a dominant global power, U.S. cyberspace policy will continue to be driven by national security issues and thus also by the military logic of deterrence. For the EU, however, questions of data protection will continue to be of central significance as long as its approach to cyberspace is police-driven and focused on improving its defensive capacities. Only if these limits are respected will mutual cooperation in cyber security policy and Internet governance find some middle ground that pays off for both sides.

Transnational: The transatlantic cyber partnership is being challenged by a number of transnational conflicts involving different perceptions of the proper state-citizen relationship. Unfortunately, these require urgent attention at a time when mutual trust between states and citizens has been eroded. Disclosures have sensitized citizens to the dangers inherent in the digital revolution. It is possible that public trust in the safety of Internet communications has been deeply shaken and that some groups will begin to demand the renationalization of information and communication technology infrastructure. In the run-up to negotiations over the Transatlantic Trade and Investment Partnership (TTIP), for example, demands for the creation of supranational legal instruments and independent mediating bodies are already being voiced. In the coming years, both the EU and the United States will have to get used to emerging countries like Brazil, India, South Africa, and Indonesia demanding the more frequent use of multilateral agreements in Internet governance within the multistakeholder process.

Transatlantic Principles and Initiatives

A transatlantic cyber partnership between the EU and the United States has developed and strengthened over the last several years. The policies of both regions share a common normative foundation and regulatory principles and are characterized by very similar domestic political debates. Both regions also share similar ideas about the most appropriate regulatory structure for the Internet.[1]

The Internet's cyberspace, as a global public space and an economic resource, is a public good. Because the Internet spans the globe, the regulatory aspirations of the cyber partnership are not limited to the transatlantic region but rather "encompass all IT systems that are data-networked on a global scale."[2] The United States and the member states of the European Union are similar in that they all have service-based economies in which a large proportion of economic activity is transacted over the Internet. Essential economic infrastructure, including that of the energy, healthcare, and transportation sectors, depends on stable communication channels. In addition, Internet usage in both economic regions has increased rapidly in recent years and exceeds usage in other regions of the world by far. About 75 percent of all European households are connected to the Internet; in North and South America, about 61 percent are connected.[3] Given these similarities, it is not surprising that the European Union is using the U.S. government's International Strategy for Cyberspace of May 2011 for guidance in the development of its own unified "cyberspace policy." Together with international partners and organizations, the private sector, and civil society, the EU wants to create a policy that helps guarantee "the preservation of an open, free and secure cyberspace" and serves to "bridge the 'digital divide'."[4]

Multistakeholder Model

Certainly the most important common feature of U.S. and EU Internet governance is the insight that the global Internet is a collective good and that its nature as a collective good depends on universal free online access.[5] Both are guided by the normative principle that citizens should be able to use the Internet to the fullest extent possible, limits being acceptable only to prevent harm to others. Moreover, the Internet should be subject to national laws only insofar as the hardware and software of information and communication technology is located within national borders.

These shared normative principles of the transatlantic cyber partnership find expression also in a shared understanding of how the Internet should be regulated. As part of the UN World Summit on the Information Society (WSIS), a dispute between China and the United States developed between 2002 and 2005 over whether the Internet should be managed by private businesses or public authorities. In response to this question, the Working Group on Internet Governance (WGIG), which had been assembled by then UN Secretary-General Kofi Annan, developed the "multistakeholder model." Supported at that time by 190 states, it acknowledges the fact that the Internet has no central governing authority but arises instead as a product of the interaction of all participating and affected stakeholders including governments, businesses, civil society actors, and the technical community. In principle, everyone can participate in the most important regulatory bodies such as the Internet Society (ISOC), the Internet Engineering Task Force (IETF), or the Internet Governance Forum (IGF). The price of participation is "not a political declaration of belief, but the ability and willingness to contribute something to the solution of practical (Internet) prob-

1 Andreas Fröhling, "Was ist Cyberdefence?," *Behörden-Spiegel*, March 2013: 70.

2 Bundesministerium des Innern, *Cyber-Sicherheitsstrategie für Deutschland* (Berlin, February 2011), 14.

3 International Telecommunication Union (ITU), *Facts and Figures. The World in 2013* (Geneva, 2013).

4 Annegret Bendiek, Marcel Dickow, and Jens Meyer, *Europäische Außenpolitik und das Netz. Orientierungspunkte für eine Cyber-Außenpolitik der EU*, SWP-Aktuell 60/2012 (Berlin: Stiftung Wissenschaft und Politik, October 2012).

5 Freedom House, *Freedom on the Net 2013* (Washington, DC/ New York, 2013), http://www.freedomhouse.org/report/ freedom-net/ freedom-net-2013; see also "Russischer Geheimdienst will komplette Internetkommunikation speichern," *Spiegel Online*, October 21, 2013.

lems."[6] The outcomes of participation should depend not on place of origin or membership in a particular electorate, but rather on the strength of argument, the innovative power of proposals, and the plausibility of misgivings. A "rough consensus" is considered to have been achieved when the major groups involved have no more fundamental objections.

The "generic Top Level Domain" (gTLD) program of the Internet Corporation for Assigned Names and Numbers (ICANN)[7] is an example of how political and economic problems can be solved in a multistakeholder process. The most convincing evidence in favor of the existing multistakeholder structure, however, is its robust growth. The number of Internet users has increased over the past 20 years to about 2 billion, and the openness of the Internet has brought forth innovative and creative applications that have made the Internet culturally diverse and economically virile.[8]

The current structure is certainly not without controversy. Authoritarian states such as China, Russia, and Iran are pushing for an Internet regime that is more directly tied to the United Nations and in which national governments again acquire broad regulatory latitude. A Western alliance consisting of the United States, EU member states, Japan, Australia, and Canada has successfully resisted such advances so far. Most of all, these countries fear that a greater role for UN bodies would increase the ability of authoritarian governments to abuse their power in intergovernmental cooperation. If the Domain Name System (DNS), for example, were no longer controlled by ICANN but rather by governments as part of the International Telecommunication Union (ITU), it could be used as an instrument of political power to lock out undesired users from the Internet. The "great firewall" of the Chinese government and the blockade of Google and other websites in the "halal" network of Iran show that this risk is not hypothetical.[9]

6 Wolfgang Kleinwächter (ed.), *Internet und Demokratie*, MIND [Multistakeholder Internet Dialog] #5; Collaboratory Discussion Paper Series, no. 1 (Berlin, June 2013), 8.
7 ICANN coordinates the Internet's systems of unique identifiers: IP addresses, protocol parameter registries, top-level domain space (DNS root zone).
8 Vint Cerf, "Reflections about the Internet and Human Rights: Video Keynote," in *Keep the Internet Free, Open and Secure*, ed. Lorena Jaume-Palasi and Wolfgang Kleinwächter (Berlin, 2013), 40f.
9 Alex Comninos, *Freedom of Peaceful Assembly and Freedom of Association and the Internet* (Melville [South Africa]: Association for Progressive Communications [APC], June 2012).

The members of the Organization for Economic Cooperation and Development (OECD) see the current Internet governance regime as a neutral arrangement. A bill that passed the Energy and Commerce Committee of the U.S. House of Representatives called for the preservation of the existing model of Internet governance and spoke out against any extension of ITU authority over the Internet.[10] Similarly, the European Parliament (EP) and the European Commission underscored their commitment to a free and open Internet at the 2012 World Conference on International Telecommunications (WCIT) in Dubai.[11] Yet both proponents and detractors of the existing multistakeholder structure know that it raises governance questions that remain unanswered. The heated debates over Internet regulation in the ITU and over the introduction of new top-level domains at ICANN demonstrate just how important a policy tool technical standardization has become. The role of national and supranational political bodies in these institutions is far from being authoritatively defined. An even more delicate situation arises when individual technical gatekeepers are themselves able to determine technical standards, as in the browser market.[12]

Domestic Debates

The domestic political debates on Internet policy in the EU and the United States are very similar. Discussion centers around how barrier-free access to digital infrastructure both in terms of geographic reach and speed (broadband infrastructure) can be achieved for as many people as possible; debates address also the issue of which restrictions on access are legitimate.

10 GauthamNagesh, "An Internet (Almost) Free from Government Control," *Roll Call*, April 17, 2013, http://www.rollcall.com/news/an_Internet_almost_free_from_government_control-224101-1.html.
11 European Commission, *Digital Agenda: EU Defends Open Internet at Dubai International Telecommunications Conference*, Memo/12/922 (Brussels, November 30, 2012); European Parliament, *Resolution on the Forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunication Union, and the Possible Expansion of the Scope of International Telecommunication Regulations*, 2012/2881(RSP) (Strasbourg, November 22, 2012).
12 Guido Brinkel, "Datenpolitik," in *Kompendium Digitale Standortpolitik*, ed. AnsgarBaums and Ben Scott, (Berlin, June 2013), 128–38 (133ff), http://www.stiftung-nv.de/mstream.ashx?g=111327&a=1&ts=635215654714766229&s=&r=-1&id=151668&lp=635076896901470000.

The European Commission presented a "digital task list" in December 2012, which made the creation of a stable regulatory environment for investment in broadband networks a top priority. The new "EU guidelines for the application of state aid rules in relation to the rapid deployment of broadband networks" has been in force since January 2013.[13] The guidelines are intended to strengthen non-discriminatory network access ("open access") so as to encourage competition in publically subsidized network infrastructures.[14]

Equally controversial in the United States and the EU is the question of network neutrality. The Federal Communications Commission (FCC) announced in 2010 that it will prohibit providers from discriminating among Internet packets during transport on the basis of their content. Europeans, too, are debating whether Internet service providers may grant content providers (such as Facebook, YouTube, or Spotify) higher transport speeds for their data as a paid service. In September 2013, Digital Agenda Commissioner Neelie Kroes introduced regulations that would provide the basis for a two-class network throughout Europe.[15] In early February 2014, House and Senate Democrats introduced a net neutrality bill. This bill, the Open Internet Preservation Act, is a response to a federal court decision that struck down the FCC's net neutrality rules, which had prevented Internet providers from blocking or slowing access to certain websites.

The principle of maximum possible access to the Internet is reflected on both sides of the Atlantic in what are known as "freedom online" strategies.[16] In May 2009, the United States launched its program for Internet freedom.[17] The EU followed in August 2012.[18] In 2012, the United States invested over $100 million in order to help ensure that opposition forces in countries with authoritarian regimes have continual, unrestricted network access using "Internet in a suitcase" technology. This is meant to prevent those in power from simply turning off the Internet in conflict situations and thus to ensure that regime opponents always have the capacity to coordinate their actions on social networks and inform the global public. In response to the Arab upheavals, the United States forged the "Freedom Online Coalition" in 2011, with then Secretary of State Hillary Clinton at its head; the coalition now includes 19 states.[19] The coalition also set itself the goal of ensuring that political activists in authoritarian states have unrestricted access to the Internet. With its "no disconnect" strategy, the EU intends to protect human rights and fundamental freedoms both online and offline, and it seeks to expand information and communication technology such as to promote political freedom, democratic development, and economic growth.[20] The EU can now finance these goals through its newly created Democracy Fund.

Cybercrime and the Budapest Convention

Despite ongoing differences in the substantive definition and prevalent usage of military terms like "cyber war," a common corpus of important distinctions and categorizations has developed.[21] Cybercrime has expanded massively in recent years on both sides of the Atlantic; it is now estimated to cost German corpora-

13 *Official Journal of the European Union*, 2013/C 25/01 (January 26, 2013).

14 Note that technologies developed by the Chinese firm Huawei are used by more than 400 telecommunications firms in more than 140 countries. Among its customers are 45 to 50 of the largest telecommunications companies worldwide. Huawei is setting up eight of the world's nine largest national broadband networks including those of Great Britain, New Zealand, Singapore, and Malaysia. "Huawei will Engagement beim Netzausbau ausweiten," *Behörden-Spiegel*, July 2012: 19.

15 European Commission, *Commission Adopts Regulatory Proposals for a Connected Continent*, Memo/13/779 (Brussels, September 11, 2013).

16 Richard Fontaine and Will Rogers, *Internet Freedom. A Foreign Policy Imperative in the Digital Age* (Washington, DC: Center for a New American Security, June 2011).

17 U.S. Department of State, *21st Century Statecraft*, May 2009; Hillary Clinton, *Remarks on Internet Freedom* (Washington, DC: U.S. Department of State, January 21, 2010); Fontaine and Rogers, *Internet Freedom* (see note 16), 11–13.

18 "European Parliament Calls for Digital Freedom," *Bulletin Quotidien Europe*, no. 10749 (December 12, 2012); European Parliament, *Draft Report on a Digital Freedom Strategy in EU Foreign Policy*, 2012/2094 (INI) (Strasbourg, August 24, 2012); Ben Wagner, "Freedom of Expression on the Internet: Implications for Foreign Policy," *Global Information Society Watch*, (2011): 20–22.

19 Guido Westerwelle, "Die Freiheit im Netz," in *Frankfurter Rundschau*, May 27, 2011; "Im Spagat zur Internetfreiheit," *Deutsche Welle*, June 20, 2013.

20 European Commission, *A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean*, Joint Communication, COM(2011) 200 final (Brussels, March 8, 2011).

21 Sandro Gaycken, "Cybersicherheitsfragen und –antworten," in *Kompendium Digitale Standortpolitik,* ed. Baums and Scott (see note 12), 178–182; also Thomas Rid, *Cyber War Will Not Take Place* (London, 2013); *A Fierce Domain: Conflict in Cyberspace. 1986 to 2012*, ed. Jason Healey (Vienna, VA, 2013).

tions alone an average of €4.8 million annually. Although this figure is lower than the €6.9 million estimated for U.S. firms, it is higher than the values for Japan (€3.9 million), Australia (€2.6 million), and the UK (€2.5 million).[22] Corporations in the U.S. sample reported 1.8 successful attacks per week and that costs incurred due to these attacks had been rising annually by about 40 percent. Crimes such as trade credit fraud and industrial espionage occur with similar frequency in Europe. The Internet has also opened up a new international space for criminal offenses. The biggest challenges for investigators in the fight against cybercrime include skimming, phishing, carding, malware, botnets, DDoS attacks, account takeovers, and underground markets like Silk Road 2.0 that utilize the virtual currency Bitcoin and are often hidden in TOR networks. These new phenomena are flexible, dynamic, expansive, and, above all, anonymous.[23]

Probably the most important document in the transatlantic fight against cybercrime is the Convention on Cybercrime, also known as the Budapest Convention,[24] which regulates the cooperation of all Council of Europe member states, the United States, Canada, Japan, and South Africa.[25] The convention is the first international treaty intended to harmonize national criminal law and criminal prosecution in the areas of Internet and Internet-related crime. It was a reaction to the problem that national provisions regarding criminally relevant behavior in the Internet are extraordinarily heterogeneous and contain numerous loopholes. Effective legal protection is also hampered by the absence of standard definitions regarding which acts are punishable by law and by the lack of agreement over whether information about suspected criminals can be shared. In this legal environment, it is not difficult for extremists to build online forums in countries that have not ratified mutual legal assistance treaties or where the issues discussed online are not criminal offenses. In closed forums, even terrorist plots can be freely discussed.

22 Ponemon Institute, *2012 Cost of Cyber Crime Study: United States* (Traverse City, MI: October 2012); also Bundesverband der Deutschen Industrie (BDI), *Sicherheit für das Industrieland Deutschland. Grundsatzpapier* (Berlin, June 2013), 10.
23 LiorTabansky, "Cybercrime: A National Security Issue?," *Military and Strategic Affairs* 4, no. 3 (December 2012): 117–36.
24 Council of Europe, *Convention on Cybercrime* (Budapest, November 23, 2001).
25 Czech Republic, Greece, Ireland, Poland and Sweden have not yet ratified the convention, Nikolaj Nielsen, "EU Seeks U.S. Help to Fight Cyber Criminals," *EUobserver*, May 2, 2012.

The convention, which went into effect in 2004, covers a wide range of criminal offenses in the attempt to compensate for these gaps. It sets criteria for ascertaining whether a crime has been committed and enumerates appropriate measures to be taken by state authorities against such breaches of the law. It encompasses fraud, child pornography, infringement of intellectual property rights, and intrusion into computer systems belonging to others. The agreement represents a major advance toward creating a common judicial area.

Despite its significance for the prosecution of cybercrime, the convention has in no way brought about complete harmonization. One stubborn point of conflict is the often insufficient implementation of the convention by its European signatories, the prime example being the difficulties some countries have experienced in making data retention legally mandatory despite the clear implications of the Budapest Convention. Another problem is the prohibition on the dissemination of racist propaganda. In a number of countries — including the United States, Russia, China, Brazil, and India — a ban is not possible because of overriding protections for the freedom of expression or because of other national legal principles.

The Military Dimension of Cyber Security and the Tallinn Manual

The so-called Tallinn Manual represents an important foundation for transatlantic cooperation in responding to militarily relevant cyber threats. The manual is designed to assist in adapting essential principles of international law to the conditions of the cyber age. At the invitation of NATO's Cooperative Cyber Defence Centre of Excellence, a group of eminent international law scholars met in Tallinn, Estonia to formulate a total of 95 guidelines for governmental reactions to cyber attacks. The first working document was published in March 2013.[26] It provides a mutual point of reference for converging and diverging European and U.S. definitions of military attack, distinctions between civilian and military targets, and methods of establishing which parties are or were involved in specific

26 *Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence*, ed. Michael N. Schmitt (Cambridge et al., 2013).

cyberspace conflicts. NATO officials describe it as "the most important legal document of the cyber era."[27]

The manual declares that, in principle, the provisions of the Charter of the United Nations are applicable to cyber attacks.[28] It appeals to nations not to treat cyberspace as a legal vacuum in which legal principles applying to physical space are invalid. On the contrary, whenever states or the international community respond to cyber attacks, they are obliged to ensure that their responses comply with the requirements of international law.[29] The document specifies when and under what conditions an act of war has been committed and what measures states may take to retaliate. Rule 13 asserts that if cyber activity crosses the threshold of an armed assault in the sense of Article 51 of the UN Charter, states should be entitled to exercise their inherent right of self-defense. In these stipulations, the manual lays the cornerstone for the principle that cyber operations, if they result in serious damage and deaths, may be answered with the weapons of real war.

The authors of the manual do not provide clear criteria by which an attack may be defined as an act of war.[30] This question, they write, must be assessed case by case in reference to the decision's potential effects and gravity. Although pure cyber espionage is not considered an act of war under the Tallinn rules, spying attacks that could be interpreted as preparation for a destructive assault certainly may be answered with a preventive strike against the spy. States may claim their right to self-defense if an attacker is a state or even an organized group, but not if the attack is initiated by an individual. Also, information leaks cannot on principle be answered militarily unless they exceed a critical threshold such that they make casualties imminently possible.

The authors of the manual also take a position on the conditions that justify preemptive action against cyber attacks,[31] allowing it when an attack is "imminent."[32] The crux of the matter, however, lies in defining "imminent." The use of Stuxnet against the Iranian nuclear program is seen, for example, by some "as an act of preventive self-defense."[33] Some authors even argue that "catastrophic" economic damage could justify retaliation and could trigger self-defense measures or Security Council sanctions under Article 39 of the UN Charter. In simulations conducted by the experts in Tallinn, a cyber attack that disrupted the New York Stock Exchange for several days was ruled to have been serious enough to justify actions of self-defense.

The Tallinn Manual is not without controversy. Critics point out that using international law to set up rules for cyber war just makes these kinds of actions seem more doable and that there is no precedent for norms that deal with conflict below the threshold of armed assault. Moreover, the exclusion from the talks of experts from non-NATO states is criticized as having limited the scope of group discussions.

Joint Transatlantic Initiatives

Times are changing for the transatlantic cyber partnership. The direction and speed of change is periodically evolving through initiatives in the context of NATO, EU-U.S. cooperation, bilateral cooperation between the United States and individual EU member states, and confidence and security building measures toward third parties.

NATO's Strategic Concept 2010 is currently the core document for transatlantic security issues. Although cyber security is a marginal theme in the paper, it is clearly of growing concern to NATO: "Cyber attacks are becoming more frequent, more organized, and more costly in the damage that they inflict on government administrations, businesses, economies, and potentially also transportation and supply networks

27 Thomas Darnstädt, Marcel Rosenbach and Gregor Peter Schmitz, "Cyberwar: Ausweitung der Kampfzone," in *Der Spiegel*, no. 14 (March 30, 2013): 76–79.

28 See further Harold Hongju Koh, *International Law in Cyberspace* (Washington, DC: U.S. Department of State, September 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm.

29 Interview with Michael Schmitt in "Das Internet ist jetzt Teil des Waffenarsenals," *New Scientist Deutschland*, April 19, 2013: 56f; Nils Melzer, "95 Thesen für den korrekten Cyberkrieg," *New Scientist Deutschland*, March 28, 2013: 6.

30 *Tallinn Manual* (see note 26), Chapter II: "The Use of Force," Section 1: "Prohibition of the Use of Force."

31 Ellen Nakashima, "In Cyberwarfare, Rules of Engagement Still Hard to Define," *The Washington Post*, March 10, 2013; John Arquilla, "Panetta's Wrong about a Cyber 'Pearl Harbor'," *Foreign Policy*, November 19, 2012.

32 *Tallinn Manual* (see note 26), Chapter II: "The Use of Force," Section 2: "Self-Defence."

33 A critical assessment provided by James A. Lewis, "In Defense of Stuxnet," *Military and Strategic Affairs* 4, no. 3 (2012): 65–76. Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (Autumn 2012): 46–70.

and other critical infrastructure."[34] Such attacks "can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability."[35] NATO concludes that military defense measures are therefore necessary and should aim to further develop the alliance's capacity to "prevent, detect, defend against, and recover from cyberattacks."[36] This necessitates building state capacities and improving cooperation among NATO member states and between these states and NATO. The Strategic Concept takes no position on the question of whether cyber attacks can be used to justify invoking Article 5 of the NATO charter (the collective defense clause) or whether cyber attacks might be met with a collective response. The vast majority of states seems to prefer leaving this question open so that each case can be decided individually in light of the specific situation.

NATO clarified its policy when it adopted its Cyber Defense Policy in June 2011 and an Action Plan three months later. With these steps, NATO has begun to build an institutionalized cyber defense structure to coordinate member states' defense plans.[37] It is striking, however, that only a few NATO member states have shown strong interest in implementing the action plan or in participating in NATO cyber exercises, and neither Britain nor France belong to the active group. In April 2013, NATO and Russia announced their intention to extend cooperation in cyber security to the NATO-Russia Council level.

The EU-U.S. Working Group on Cyber Security and Cyber Crime was established in November 2010. It is addressing the fact that in many cases cyber attacks cannot immediately be attributed to a specific actor; this often requires a long "forensic" investigation, and sometimes the real perpetrator is never found. The first joint exercise of the EU and the United States, in November 2011, ("Cyber Atlantic 2011") was designed to improve coordination and provide a more detailed analysis of vulnerabilities. Based on its results, the EU held its second European cyber security exercise ("Cyber Europe 2012"), in which more than 500 experts from 29 EU/EFTA states participated. The goals of the exercise were to make critical national and European infrastructure more robust and to strengthen cooperation, preparedness, and response capability in case of a cyber security event. The Working Group is planning a joint "month of cyber security" in 2014 during which the coordination of U.S. and EU defense mechanisms is to be improved.

Cooperation in Trust-Building Measures

In many areas, cyberspace policy has direct military relevance. With the goal of preventing a new arms race in cyberspace policy, since 2011, the EU and the United States have launched a number of joint initiatives to establish confidence and security building measures in relations with Russia and China. Discussions about these measures have been conducted in the United Nations, the Organization for Security and Cooperation in Europe (OSCE), the G8, and in several conferences including the Munich Security Conference, the London Conference on Cyberspace with follow-up events in Budapest and Seoul, and the Berlin Conference on International Cyber Security. International organizations and forums also address themselves to cyber security, including the OECD, the ITU Global Cyber Security Agenda, the Internet Governance Forum (established in the wake of the UN World Summit on the Information Society), and the G20. These discussions are taking place in an environment characterized by fundamentally different views about the appropriate objectives of cyberspace regulation. EU member states and the United States place great emphasis on unrestricted access to cyberspace and on the freedom of its content and use. Russia, China, and other authoritarian states, however, are much more interested in tighter controls.[38] In authoritarian states, "cyber security" means suppressing politically undesired content and creating new tools to repress dissidents; the development and implementation of confidence and security building measures are often handicapped by these objectives, which are diametrically opposed to the goals of the transatlantic partnership. For the EU and the United States, access to cyberspace and the freedom of its content and use — within the limits of legal and democratic principles — remain the central reference points for judging the value of

34 NATO, *Active Engagement, Modern Defence* (Lisbon, November 20, 2010), 11.

35 Ibid.

36 Ibid., 16.

37 "Nato/Defence: Nato Prepares Roadmap for Cyber-Defence," *Europe Diplomacy &Defence*, no. 587 (February 26, 2013); Gerd Lehmann, "Schlüssel zum Erfolg. Kohärentes Führungs- und Aufklärungssystem für NATO und EU," *Behörden-Spiegel* (December 2011): 54.

38 For more details on the differing positions see *citizenlab.org*. For the U.S. perspective, see Richard A. Clarke and Robert K. Knake, *Cyber War* (New York, 2010), Chapter 7.

security measures. Such measures must show deference to the goal of responsible and reasonable state action in cyberspace and sensitivity to the tension between security in cyberspace and freedom of information.

Multilateral international treaties akin to those used for disarmament and arms control are currently unfeasible in the area of cyber security because of elementary differences separating the United States and Europe from Russia and China over the use of military operations in cyberspace.[39] Their differences are entrenched in several areas: implementation and verification, the definition of cyber weapons, and the attribution of attacks under international law or national criminal law. EU member states are working closely with the United States, Canada, Japan, and Australia in the UN and in the OSCE to develop a code of conduct for state behavior in cyberspace.[40] A group of 15 government representatives was given a mandate to this end from the UN General Assembly. It submitted a final report on responsible state behavior in cyberspace to the 68th General Assembly in June 2013; the group also proposed confidence and security building measures. At the same time, bilateral dialogues are booming as a way of cutting through the profound differences separating democratic and authoritarian states.[41] The United States and Germany have separately entered into special agreements with Russia and have started talks with China. These exchanges focus on priority-setting within risk assessment procedures and the standards and norms for state behavior in cyberspace currently being negotiated in the UN GGE (Group of Governmental Experts of the United Nations).[42] Here, too, however, serious differences are evident. Russia wants to outlaw the use of cyber weapons in general.[43] The United States does not. Assumedly, the U.S. position is motivated by its technical superiority in the area and the difficulty of reliably monitoring compliance with such agreements.

39 James A. Lewis, "Multilateral Agreements to Constrain Cyberconflict,"*Arms Control Today*40, no. 5 (June 2010): 14–19.
40 Tim Maurer, *Cyber Norm Emergence at the United Nations. An Analysis of the UN's Activities Regarding Cyber-security* (Cambridge, MA: Belfer Center for Science and International Affairs, September 2011).
41 "Russia, U.S. Will Try to Reach Agreements on Rules Governing Information Security – Newspaper," *Interfax*, April 29, 2013; "U.S., China Discuss Cyber Security as Dialogue Begins," *Voice of America*, July 9, 2013.
42 Jane Perlez, "U.S. and China Put Focus on Cybersecurity," *The New York Times*, April 22, 2013.
43 Rex Hughes, "A Treaty for Cyberspace," *International Affairs* 86, no. 2 (2010): 523–41. *Draft Convention on International Information Security* (Yekaterinburg, September 2011).

Areas of Conflict

In spite of wide areas of consensus between the United States and EU member states regarding the norms and principles that should govern cyberspace and the Internet, the transatlantic relationship is still hectored by serious conflicts. These include different ideas about the best mode of global Internet governance (global conflicts), very different cyber security concepts for the transatlantic partnership (transatlantic conflicts), and disruptions in the regulation of relations between states and citizens due to actions taken by partner nations (transnational conflicts). A separate matter, important but not covered here, is the U.K.'s reservations about what it sees as an overly harmonized approach to interior and justice policy within the EU and the impact of the British position on transatlantic cooperation.

Global Conflicts

The Multistakeholder Approach

A first important point of conflict emerged around the pre-existing multistakeholder model of Internet governance. Several emerging high-growth countries — including Brazil, India, South Africa, Turkey, and Indonesia — consider themselves to be insufficiently represented in organizations such as ICANN and IGF, and are pressing for a greater role for intergovernmental bodies such as the ITU. To date, the ITU has limited itself to standardization and building technical capacity in developing countries. Its mandate was basically limited to the management of the treaty on International Telecommunication Regulations (ITR), by which the global interconnection and interoperability of the telephone system is ensured. During the World Conference on International Telecommunications (WCIT) in December 2012 in Dubai, a conflict escalated between the United States, Europe, and other Western countries and the IBSA/BRICS nations. The latter demanded that the ITR contract be renegotiated, with the goal of extending its reach to the Internet and significantly expanding the powers of the intergovernmental ITU.[44] Their intention was to break U.S. hegemony in the management of the Internet and to create a new order in which the states of the south would have more weight.

These demands were met with little enthusiasm by the United States, Europe, Japan, Australia, and Canada. The Western states refused to call the multistakeholder model into question or to outfit the ITU with new powers. They even rejected a modest compromise proposal to append to the ITR some general statements about the "cooperation of governments on spam" and "network security" as well as a non-binding declaration on the involvement of the ITU in Internet regulation.[45]

On the heels of Edward Snowden's revelations in the summer of 2013, some cracks seem to have emerged for the first time in the wall put up by Western states to prevent a reorganization of Internet governance. The EU has not dropped its support of the multistakeholder approach, but its insistence on a more comprehensive inclusion of democratic countries such as Brazil and India has become more urgent, as seen in EU Commissioner Neelie Kroes' recent demand for greater inclusivity and transparency.[46] She argued that past practice, characterized by the unilateral dominance of the United States and its allies in bodies such as ICANN, needs to be corrected. Unlike the United States, the EU seeks to strengthen the Governmental Advisory Committee (GAC) of ICANN and with it the principle of intergovernmentalism. In June 2013, the European Commission also proposed to set up a Global Internet Policy Observatory in cooperation with Brazil, the African Union, Switzerland, and some non-governmental organizations. Its goal is to provide

44 Ben Scott and Tim Maurer, "Digitale Entwicklungspolitik," in *Kompendium Digitale Standortpolitik*, ed. Baums and Scott (see note 12), 126f; Hannes Ebert and Tim Maurer, "Contested Cyberspace and Rising Powers," *Third World Quarterly* 34, no. 6 (2013): 1054–1074.

45 Tim Maurer, *What Is at Stake at WCIT? An Overview of WCIT and the ITU's Role in Internet Governance* (Washington, DC: New America Foundation, Open Technology Institute, December 5, 2012); Isabel Skierka, "Kampf um die Netzherrschaft," *Adlas – Magazin für Außen- und Sicherheitspolitik* 7, no. 1 (2013): 12–16.

46 Neelie Kroes, *Building a Connected Continent*, SPEECH/13/741 (Brussels: European Commission, September 24, 2013).

more transparency and open up new avenues of participation in Internet governance.

Brazil and Germany have proposed supplementing and expanding the International Covenant on Civil and Political Rights — adopted by the UN in 1966 and in force since 1976 — for the digital world. An overwhelming majority of the 193 UN member states support this initiative. Regardless of the inherent value of such initiatives and whether they have a real chance of changing existing structures of Internet governance, it is becoming very clear that not only the EU but also other countries such as Brazil, India, Turkey, and Indonesia will increase pressure on the United States and that demands for an order that is more inclusive for emerging democracies can no longer be brushed aside.[47]

Technological Sovereignty

Snowden's disclosures not only bolstered calls for a reorganization of Internet governance, they also set off a push for stricter national control of communications infrastructures. To this end, the European Commission put forward a strategy for "Unleashing the potential of cloud computing in Europe" in September 2012.[48] Although this initiative was originally primarily intended to create jobs, after U.S. surveillance practices became common knowledge, the issue of "data sovereignty" was pushed to the fore. The cloud computing strategy envisages further harmonization in the technical standards used by member states. In addition, it calls for an EU-wide certification system for trusted cloud providers and for model drafts of secure and fair contracts. The Commission favors the establishment of a European Cloud Partnership linking member states and the computing industry, in order to better utilize public power over the sector's markets. The goal is to strengthen European cloud providers, helping them achieve efficiencies of scale and compete more successfully with their U.S. competitors.

The European Commission believes that an EU-wide cloud computing system is needed to protect European public authorities and private companies from espionage. Files that are stored on cloud platforms such as Dropbox, Google Drive, or Skydrive can become a serious security problem. Typical dangers lurk in servers that are physically located outside Europe; and also in the wording of general terms and conditions, which often gives quite far-reaching access rights to server providers. Under these conditions, U.S. authorities can easily gain access to the data of Europeans who use the cloud-computing services of companies like Google, Facebook, or Dropbox. Finally, theft of private content, like that recently experienced by Dropbox, cannot be completely ruled out.

The European Parliament's Committee on Civil Liberties, Justice, and Home Affairs commissioned a study in 2012 that showed that cloud computing is a relevant security risk, particularly when data is stored on the servers of U.S. providers.[49] Law scholars of the University of Amsterdam pointed out in November 2012 that the Patriot Act gives U.S. intelligence agencies extensive access rights to communications and user data.[50] On the basis of the Patriot Act and the Foreign Intelligence Surveillance Amendments Act (FISAA) of 2008, which was extended to 2017, U.S. investigators may request a secret court authorization to monitor foreign users. The laws require U.S. cloud providers such as Google or Amazon to release customer data on request, optionally with the obligation to keep the transaction secret, regardless of whether this data is stored on servers located in Europe or the United States. These rules apply also to European firms doing business in the United States. The authors of the EP study recommended giving top priority to legal certainty in cloud computing. The EU's objective, they write, should be to place at least 50 percent of EU services offered from cloud computers within the jurisdiction of EU law by the year 2020.[51]

In Germany, the concept of technological sovereignty has been circulating for some years and has had active supporters in the government. For example, German Interior Minister Thomas de Maizière made a point of campaigning for technological sovereignty in

47 Internet Governance Project (IGP), *Comments of the Internet Governance Project on the ICANN Transition*, June 2009; IGP, *The Core Internet Institutions Abandon the U.S. Government*, October 11, 2013.

48 European Commission, *Unleashing the Potential of Cloud Computing in Europe*, COM (2012) 529 final (Brussels, September 27, 2012).

49 Didier Bigo et al., *Fighting Cyber Crime and Protecting Privacy in the Cloud* (Brussels: EP, October 2012); Didier Bigo et al., *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law* (Brussels: EP, October 2013).

50 J. V. J. van Hoboken et al., *Cloud Computing in Higher Education and Research Institutions and the United States Patriot Act* (Amsterdam: Institute for Information Law, November 2012).

51 Bigo et al., *Fighting Cyber Crime* (see note 49), 50.

June 2010.[52] The German federal government outlined an initial response to U.S. espionage activities in an eight-point plan presented in July 2013. This set of measures is supposed to help facilitate new security standards and improve access to venture capital for entrepreneurs interested in providing secure online services based on European data protection guidelines. At the European level, too, the government supports an ambitious IT strategy to promote Internet-based business models that are sensitive to issues of user security. New start-ups are to be encouraged and supported financially. The debate over the technology policy implications of the NSA's activity also led Deutsche Telekom's idea of "Schengen Routing."

A global paradigm shift in information and communication technology is taking shape as confidence in the free interplay of market forces has been shaken and, for the first time in the digital age, the physical location of a company's headquarters has become a decisive criterion of IT system security. Trustworthiness is the issue now, and "foreign" companies are treated with suspicion. Attention is drawn to the preponderance of U.S. firms among the world's IT companies and to the fact that most IT equipment is manufactured in Asia. The solution for countering these monopolies would seem to be the creation of "national" technologies.

Transatlantic Conflicts

The cyber security policy of the United States and the EU is characterized by two very different basic ideas. In the United States, the logic of military defense and deterrence dominates. For Europeans, security lies squarely in the purview of police authorities and, where present, Computer Emergency Response Teams (CERTs), whose central goal is strengthening domestic capacities to recover from cyber attacks (resilience) or resist them in the first place.

U.S. Strategy: Toward Cyber Deterrence

Cyber defense and deterrence is of central importance to the United States and is coordinated by the Pentagon's United States Cyber Command (USCYBERCOM), which was created in 2010 and has about 900 employees. Cyber Command is located in Fort Meade, Maryland, also the headquarters of the National Security Agency (NSA), the largest U.S. intelligence agency, and shares a double-hatted commander with the NSA. Reporting to the United States Strategic Command (USSTRATCOM), Cyber Command's mandate is to coordinate defense operations against potential attacks (Computer Network Defense) and at the same time to build an offensive attack capability (Cyber Attack Operations).[53] The fact that Cyber Command employees are to be quintupled to about 4,900 gives some indication of the importance the United States places on these measures. Thirteen cyber attack teams are to be formed for carrying out so-called cyber-kinetic attacks, i.e., cyber attacks that destroy objects.[54]

The outstanding importance of the security agenda is also reflected in its financial resources. The Pentagon requested $4.7 billion for operations in this area in 2014, about $1 billion more than in 2013. Over the next four years, another $23 billion is to be spent.[55] For their work, the U.S. government budgeted a total of $52.6 billion for the fiscal year 2013, as Edward Snowden revealed to *The Washington Post*.[56] The largest amount, $14.7 billion, was requested by the Central Intelligence Agency (CIA). The NSA, which specializes in electronic communications spying, put in the second largest request of $10.8 billion. The National Reconnaissance Office (NRO), responsible for spy satellites, had the third largest request with $10.3 billion. Together, these three agencies were responsible for two-thirds of the intelligence budget.

According to news magazine *Der Spiegel*,[57] the NSA and CIA operate secret listening posts, internally referred to as the Special Collection Service (SCS), in

52 Thomas de Maizière, *14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft* (Berlin: Bundesministerium des Innern, June 22, 2010).

53 James Bamford, *The Shadow Factory. The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York, 2008).

54 "Pentagon Reviews 'Rules of Engagement' against Cyber Attacks," *Europe Diplomacy &Defence*, no. 620 (July 4, 2013).

55 James Bamford, "The Secret War. Infiltration. Sabotage. Mayhem. For Years, Four Star General Keith Alexander Has Been Building A Secret Army Capable of Launching Devastating Cyberattacks," *Wired*, June 12, 2013.

56 Barton Gellman and Greg Miller, "U.S. Spy Network's Successes, Failures and Objectives Detailed in 'Black Budget' Summary," *The Washington Post*, August 29, 2013, http://www.washingtonpost.com/wp-srv/special/national/black-budget/.

57 "Embassy Espionage: The NSA's Secret Spy Hub in Berlin," *Der Spiegel*, October 17, 2013, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

about 80 U.S. embassies and consulates. The small SCS teams collect communications in their respective host countries from bases in various diplomatic missions. This type of technical reconnaissance is known within the NSA by the codename "stateroom."

The cyber security policy of the United States is driven by the perception, which pervades government at all levels, that national security is under threat and that this threat must be countered by military strategy and military means by building "cyberpower":

> ... the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain. Cyberpower can be used to produce preferred outcomes within cyberspace, or it can use cybersinstruments to produce preferred outcomes within cyberspace, or it can use cyberinstruments to produce preferred outcomes in other domains outside cyberspace.[58]

Just two years after the attacks of September 11, 2001, the White House published its National Strategy to Secure Cyberspace.[59] At that time, it positioned U.S. cyber security policy in the context of anti-terror measures and addressed itself specifically to the threat posed by non-state actors.[60] Over the next few years, however, this view became relativized by additional analyses of the cyber risks posed by China and Russia.

The key elements of current U.S. cyber security policy are deterrence and building a credible threat of massive retaliation.[61] In May 2011, the United States published its International Strategy for Cyberspace, in which it leaves no doubt that it will respond to any hostile act in cyberspace with appropriate countermeasures: "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."[62] Only two months later, the Department of Defense announced that attacks on critical infrastructure in the United States will trigger reprisals.[63] The then Secretary of Defense Leon Panetta warned that the United States risked a "cyber Pearl Harbor" if it did not expand its defenses.[64] In the words of former Marine Corps general and vice chairman of the Joint Chiefs of Staff James Cartwright, author of the Pentagon's current cyber strategy, "we really need to frighten our enemies."[65]

Deterrence against attacks from cyberspace is highly controversial, both in the literature and in political discussions. Many experts argue that because attackers often cannot be identified unequivocally, deterrence does not work. Even the United States government has officially stated that it expects to be able to trace only one-third of cyber attacks to a particular source.[66] A report by U.S. cyber security company Mandiant, however, claims that U.S. intelligence and military organizations know far more about the clandestine activities of potential attackers than they admit publicly.[67] The U.S.-China Economic and Security Review Commission recommended strongly in its November 2013 report to Congress that the U.S. government respond comprehensively to Chinese cyber espionage. The commission is considering trade restrictions, bans on travel to the United States for organizations with contacts to hackers, and freezing the funds of companies that use intellectual property stolen by cyber espionage. Existing sanctions could be intensified.[68]

This approach is based on the assumption that basic mechanisms of deterrence also work in the

58 Joseph S. Nye, *The Future of Power* (New York, 2011), Chapter 5. A critical assessment on "deterrence" written by Stevens, "A Cyberwar of Ideas?"

59 Neil Robinson et al., *Cyber-security Threat Characterisation. A Rapid Comparative Analysis* (Cambridge: RAND Europe, 2013), 28–32.

60 Joseph S. Nye, "What Is It That We Really Know about Cyber Conflict?," *The Daily Star*, April 24, 2012.

61 Center for Strategic and International Studies (CSIS), *Cybersecurity Two Years Later. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, DC, January 2011).

62 The White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (Washington, DC, May 2011).

63 Thomas M. Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, September 2013).

64 Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *TheNew York Times*, October 11, 2012.

65 Original quote in Darnstädt, Rosenbach and Schmitz, "Cyberwar" (see note 27).

66 Original quote in "Sicherheitsexperte Lewis über Cyber-Krieg: 'Wir müssen unsere Verteidigung stärken'" (Interview with James Lewis), *Süddeutsche Zeitung*, February 5, 2012, 16.

67 *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013).

68 U.S.-China Economic and Security Review Commission, *2013 Annual Report to Congress* (Washington, DC, November 20, 2013), http://www.uscc.gov/Annual_Reports/2013-annual-report-congress.

digital age.[69] Initial proposals for a cyber deterrence strategy include expanding military strength, building and maintaining a first-strike capacity, and upholding the possibility of responding militarily to a cyber attack in near real-time.[70] The technological and scientific dominance of the United States must be preserved by building these capacities. The United States must be able to quickly identify the goals and motives of potential attackers and must be able to take appropriate countermeasures. That U.S. cyber security measures are not merely defensive is clearly seen in the fact that the U.S. intelligence community launched 231 offensive cyber operations in 2011 alone. A $652 million project code-named GENIE employed 1,870 computer specialists to penetrate foreign networks.[71]

EU Strategy: Building Defensive Capacity and Fighting Crime

Europeans take a fundamentally different approach to cyber security, focusing on building capacities to resist cyber attacks, to recover after attacks take place (resilience), and to combat crime. EU policy has four major components that find articulation in various forms and contexts: the 2013 Cyber Security Strategy presented by the European Commission and the European External Action Service, the draft directive for Network and Information Security (NIS), the European Cybercrime Centre (EC3), and several projects designed to boost resistance and resilience capacities.

The European Cyber Security Strategy[72] was adopted in June 2013. It aims to ensure the security of information technologies and to guard fundamental European rights and values. The expansion of military and intelligence capabilities are of subordinate importance, being mentioned as only one of five main planks of the strategy. The other four planks relate to the improvement of non-military capacities: resistance to cyber attacks, containment of cyber crime, expansion of industrial and technical resources for cyber security, and the formulation of a unified strategy for cyberspace.[73]

In the accompanying directive for network and information security, which has not yet been adopted, the European Commission calls on private sector enterprises to play a significant role. In its view, not only member states but also private operators have a duty to protect critical digital infrastructure. Companies should ensure that their products and services always meet certain security standards and are shielded against attacks as well as possible.[74] The cost of installing secure infrastructure for the exchange of information between member states is estimated at €10 million annually. In June 2013, the EU began to require communications companies that offer electronic communications services "to notify the competent national authorities, and in certain cases also the subscribers and individuals concerned, of personal data breaches."[75]

The EU's efforts to bolster cyber crime fighting are reflected in the expansion of its new European Cyber Crime Centre (EC3). The center is to provide analysis and information, assist in investigations, perform forensic work, facilitate cooperation among member states, inform the private sector and other actors, and eventually function as a spokesman for European law enforcement as a whole. In its first year, the EC3 as-

69 Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy* 33, no. 1 (2012): 148–70; Paul-Anton Krüger, "Digitale Abschreckung. Die United States sind bereit, Cyberangriffe mit aller Härte zu beantworten," *Süddeutsche Zeitung*, February 21, 2013, 4.

70 Frank J. Cilluffo, Sharon L. Cardash and George C. Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strength," *Military and Strategic Affairs* 4, no. 3 (2012): 3–23.

71 Barton Gellman and Ellen Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show," *The Washington Post*, August 30, 2013, http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

72 Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik, *Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final (Brussels, February 7, 2013).

73 Patryk Pawlak, *Cyber World: Site under Construction* (Paris: European Union Institute for Security Studies [EUISS], September 2013); Annegret Bendiek, *European Cyber Security Policy*, SWP Research Paper 13/2012 (Berlin: Stiftung Wissenschaft und Politik, October 2012).

74 Annegret Bendiek, *Kritische Infrastrukturen, Cybersicherheit, Datenschutz. Die EU schlägt Pflöcke für digitale Standortpolitik ein*, SWP-Aktuell 35/2013 (Berlin: Stiftung Wissenschaft und Politik, June 2013). U.S. Securities and Exchange Commission, *Disclosure Guidance* (Washington, DC, July 16, 2013), http://www.sec.gov/divisions/corpfin/cfdisclosure.shtml.

75 "Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications," *Official Journal of the European Union*, L 173, 26/06/2013 P. 0002-0008.

sisted in the coordination of 19 major cybercrime operations.[76]

Other EU measures include a pilot project to combat botnets and malware, launched in early 2013 with a €15 million budget, and financial support for critical infrastructures that link member states' NIS capacities (the Connecting Europe Facility). The objective of these measures is comprehensive protection for assets and people, especially through public-private partnerships such as the European Public-Private Partnership for Resilience (EP3R) and Trust in Digital Life (TDL). Their work is to focus on supply chain security and to integrate relevant work being conducted by the European standardization organizations (Comité Européen de Normalisation, CEN; Comité Européen de Coordination des Normes Électriques, CENELEC; European Telecommunications Standards Institute, ETSI), the Cyber Security Coordination Group (CSCG), the European Network and Information Security Agency (ENISA), the European Commission, and other actors involved. Moreover, the Framework Program "Horizon 2020" has been set up to finance the development of tools to combat criminal and terrorist activities in cyberspace and support work on security research using new information and communication technology. The EU's next multiannual financial framework for the period 2014–2020 includes about €80 billion for "Horizon 2020," making it the EU's largest ever research program. About €1.5 billion is earmarked for security research, and €400 million will go to research on cyber security.

Protection of Critical Infrastructure

The U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported in July 2012 that the number of cyber attacks on critical infrastructure in the United States increased from 9 in 2009 to 198 in 2011.[77] It its first report of January 2013, ENISA also pointed to the growing risk of cyber attacks on critical infrastructure.[78] However, the cyber security situation in Europe is still quite muddled. An obligation to report security incidents is currently being discussed in the EU and Germany (as in the United States). In the absence of officially collected statistics, sporadically published national[79] or private[80] threat analyses represent the best available standard of reporting. This is something of a handicap, as the exchange of reliable information between business, industry, public authorities, and security organizations is thought to be a central resource in the fight against cybercrime and for the protection of critical infrastructure.

In the United States, debates about cyber security over the past two years have increasingly focused on the protection of critical infrastructures and on the role of private enterprise.[81] After a U.S. Senate initiative to regulate the exchange of information on cyber threats was blocked by the House of Representatives, U.S. President Barack Obama issued an executive order on February 12, 2013[82] requesting businesses to voluntarily inform government agencies of cyber attacks.[83] Michael Daniel, cyber security officer at the White House, announced in February 2013 his intention to have the failed 2012 bill for the protection of critical infrastructure reintroduced. In the same month, President Obama gathered representatives of leading U.S. companies — including UPS, JP Morgan Chase, and Exxon Mobil — to discuss cyber threats. The president is dependent on voluntary cooperation because digital infrastructure in the United States is operated privately. In preparation for its legislative relaunch, the administration published the Cyber Security Framework (CSF) "of standards, guidelines, and best practices to promote the protection of critical infrastructure" in August 2013. The framework recommends mandatory protection standards, and was brought forward as a basis for discussion by the National Institute

76 European Commission, "European Cybercrime Centre – one year on," Press Release, February 10, 2014, http://europa.eu/rapid/press-release_IP-14-129_en.htm.
77 "Sharp Increase in Cyberattacks on U.S. Critical Infrastructure," *Homeland Security News Wire*, July 3, 2012.
78 "ENISA Reports on Most Frequent Cyber Threats in 2013," *Bulletin Quotidien Europe*, no. 10759 (9 January 2013); Louis Marinos and Andreas Sfakianakis, *ENISA Threat Landscape* (Heraklion, January 8, 2013).
79 See also "ENISA Reports on Most Frequent Cyber Threats" (see note 78); Deutsche Telekom/T-Systems (ed.), *Cyber Security Report 2012. Ergebnisse einer repräsentativen Befragung von Entscheidungsträgern aus Wirtschaft und Politik* (Bodman am Bodensee 2012).
80 See for instance the website www.sicherheitstacho.eu.
81 U.S. Department of Homeland Security, *The Strategic National Risk Assessment in Support of PPD 8: a Comprehensive Risk-based Approach toward a Secure and Resilient Nation* (Washington, DC, December 2011).
82 The White House, *Executive Order: Improving Critical Infrastructure Cybersecurity* (Washington, DC, February 12, 2013).
83 U.S. Department of Homeland Security, *National Infrastructure Protection Plan. Partnering to Enhance Protection and Resiliency* (Washington, DC, 2009), http://www.dhs.gov/national-infrastructure-protection-plan.

of Standards and Technology after consultation with stakeholders from industry, academia, and government.[84]The credit card breaches at the retailers Target, Neiman Marcus, and Michaels resurrected the push for a national data breach disclosure law in early February 2014. Senate Commerce Committee Chairman Jay Rockefeller initiated a federal breach disclosure plan. Under the so-called Data Security and Breach Notification Act, "the Federal Trade Commission (FTC) would issue security standards for businesses that hold people's personal and financial data. If those companies are hacked, they would be required to notify affected customers so they can take preventive steps on their own. Businesses would also be given incentives to adopt new technologies to make customers' data unreadable or unusable if stolen."[85]

The EU's goal of achieving unitary, binding regulation is shared by the Obama administration and the U.S. Senate but not by the House majority.[86] The current proposal for a Commission directive proposes to require operators of critical infrastructure both to protect the information technology they use and to optimize communications with regulatory agencies. For the Commission, critical infrastructure includes not only the energy and transportation sectors but also search engines, cloud computing services, social networking, Internet payment gateways, and online application markets (app stores). All of these companies are to be subject to new requirements on the reporting of IT security incidents for the purpose of increasing the efficiency of cybercrime fighting. The confidentiality of this information is to be guaranteed by the ENISA at the European level and by national information security authorities of the member states.

Data Protection

Interpretations of the proper relationship between security and freedom vary widely on both sides of the Atlantic and within the EU.[87] September 11, 2001 was a profound shock to the Americans, but the shock to the Spanish was no less after the terrorist attacks in Madrid in 2004 or to the British in the wake of the London attacks in July 2005. Yet, the experiences of other European countries with international and Islamic terrorism are different, and these different experiences influence their respective approaches and the means they consider acceptable for use in the fight against terrorism. There is wide disagreement about the conditions that would allow government authorities to access private data in the fight against organized crime or terrorism and on the issue of how long personal data may be used for other purposes than criminal investigations, if at all.

The relatively high priority given to national security issues in the United States becomes very clear in recent disclosures of the monitoring operations of the NSA (such as PRISM, Upstream, Xkeyscore, or Bullrun). The U.S. government has established a comprehensive military-industrial security architecture in the past decade and has given its intelligence agencies wide discretion to collect any information they consider relevant. The fact that the president of the United States, perhaps unwittingly, ordered the wiretapping of government offices of the EU and its member states, even going to the extreme of monitoring the conversations of heads of government, is only the most obvious expression of a security practice that seems to have lost a sense of proportion.

The Unites States still seems to be disregarding the political costs of spying on its allies. The monitoring program PRISM is defended by the Obama administration on the grounds that it used only for the collection of specific kinds of meta-data and content on specific persons, groups, and events. Additionally, it argues that all such measures are regulated under the Foreign Intelligence Surveillance Act (FISA), are subject to judicial review by the United States Foreign Intelligence Surveillance Court (FISA Court), and have to be reported to Congress.[88] And at any rate, so the argument goes, U.S. practice is hardly any different from comparable activities of Europe's own intelli-

84 National Institute of Standards, *Discussion Draft of the Preliminary Cybersecurity Framework*, August 28, 2013, http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-frame work-082813.pdf (accessed October 30, 2013);http://beta.congress.gov/bill/113th/house-bill/3696.

85 http://thehill.com/blogs/hillicon-valley/technology/197000-senate-dems-unveil-data-security-bill

86 Bendiek, *Kritische Infrastrukturen* (see note 74).

87 Jim Harper and Axel Spies, *A Reasonable Expectation of Privacy? Data Protection in the United States and Germany*, AICGS Policy Report no. 22 (Washington, DC: American Institute for Contemporary German Studies [AICGS], 2006); Quirine Eijkman and Daan Weggemans, "Open Source Intelligence and Privacy Dilemmas: Is It Time to Reassess State Accountability?," *Security and Human Rights*, no. 4 (2012): 285–96.

88 Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Washington, DC, June 8, 2013).

gence services.[89] It remains to be seen in how far the executive order to reform U.S. intelligence policy, introduced by President Obama in January 2014 and based on the 46 reform proposals submitted by his own review panel, will be implemented in the coming months.[90]

Resentment against U.S. surveillance practices has continued to rise in the EU, especially in Germany. Working Party 29 of the EU, an intergovernmental working group of data protection officers of the EU and its member states created in the mid-1990s, is currently investigating whether the United States has violated international legal norms or the Budapest Convention.[91]

The management and use of personal data has been another source of dispute between the EU and the United States for years. The issue was hotly debated in the context of agreements over the transfer of flight passenger information (Passenger Name Record or PNR) to U.S. agencies and over the exchange of financial data through the SWIFT system as part of the Terrorist Finance Tracking Program (TFTP).[92] Members of parliament have continually cited problems in the implementation of the SWIFT agreement, with some even calling for a suspension of the agreement. The European Parliament warned in a resolution that personal data must be protected and that Europe's high standards of protection must not be compromised.[93]

European negotiators discussing the Transatlantic Trade and Investment Partnership (TTIP) were urged to be on guard against the undermining of EU data protection standards. Reforms of the data privacy policy of 1995, now under discussion, would prohibit the transfer of personal data from EU member states to countries that do not have privacy protections comparable to those of the European Union. This would include the United States. At the same time, however, under the "Safe Harbor Framework," a data protection agreement signed in 2000 by the EU and the United States, U.S. companies may process European data in the United States if they pledge to uphold "safe harbor principles." In an investigation from September 2013, the Australian data protection consulting firm Galexia found that the agreement's stipulations are often ignored by U.S. companies who have pledged compliance. It identified 427 violations of the agreement among the nearly 3,000 self-certifying U.S. firms investigated; an earlier study from 2008 had found only 200.[94] The Safe Harbor Framework covers trade and economic issues relevant for data protection and is therefore treated separately from the EU-U.S. agreements that are integrated into national criminal law, including PNR, SWIFT, and legal assistance treaties.

In the new draft of EU General Data Protection Regulation, the EP has again introduced the so-called anti-FISA clause that previously had been deleted by the Commission under pressure from the U.S. government.[95] The clause would prevent businesses from providing sensitive data on EU citizens to foreign security agencies unless the transfer is covered by a mutual legal assistance treaty. Thus, as long as the United States and the EU are in disagreement on new rules for the exchange of personal data, firms operating in the United States would have to refuse requests from the U.S. government for data on EU citizens. Such legal uncertainty puts U.S. companies in a bind. In February 2014, Facebook, Yahoo, Google, LinkedIn, and Microsoft all revealed that the government had asked them for users' data. Certainly aware of this situation, the EP and the justice ministers of the member states want to adopt a final draft for the new Data Protection Regulation before 2015 that could come into effect in 2016. Viviane Reding, EU commissioner for justice, fundamental rights, and citizenship, favors the development of a European data protection system with four essential components. First, the territorial scope of regulations should be clearly and expansively defined such that non-European compa-

89 Georg Mascolo and Ben Scott, *Lessons from the Summer of Snowden. The Hard Road Back to Trust* (Washington, DC: Open Technology Institute/Wilson Center, October 2013).

90 David E. Sanger and Charlie Savage, "Obama Panel Recommends New Limits on N.S.A. Spying," *TheNew York Times*, December 18, 2013, http://www.nytimes.com/2013/12/19/us/politics/report-on-nsa-surveillance-tactics.html.

91 "Article 29 Group to Carry Out Its Own Espionage Investigation," *Bulletin Quotidien Europe*, no. 10903 (August 21, 2013).

92 Annegret Bendiek, *An den Grenzen des Rechtsstaates: EU-United States-Terrorismusbekämpfung*, SWP-Studie 3/2011 (Berlin: Stiftung Wissenschaft und Politik, February 2011).

93 Sophie in 't Veld and Guy Verhofstadt, "Europe Must Get Tough with the U.S. over NSA Spying Revelations," *The Guardian*, July 2, 2013.

94 Chris Connolly, *The U.S. Safe Harbor – Fact or Fiction?* (Sydney: Galexia, December 2008); Chris Connolly, *EU/U.S. Safe Harbor – Effectiveness of the Framework in Relation to National Security Surveillance*, October 7, 2013 (Paper for the Hearing in the LIBE Committee).

95 European Centre for International Political Economy, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, March 2013.

nies must be required to comply fully with European rules if they want to offer products and services in the European market. "If you want to play in our yard, you have to play by our rules," said Reding.[96] Second, the concept of personal data, too, should be expanded to include not only the content of e-mails and telephone calls but also traffic data pertaining to that content. Third, these rules should apply not only to companies that collect data from citizens, but also to companies that process data such as cloud providers. Finally, there must be protection against unrestricted international data transfers. Data of EU citizens should be given to non-European law enforcement agencies only under clearly defined and exceptional circumstances and only if subject to judicial review.

Negotiations over an umbrella agreement between the EU and the United States on the modalities of data protection have resumed. Europeans want such an agreement to result in the strengthening of citizens' rights to access, correct, and delete their own data. Also, it should grant EU citizens a right of legal redress if their data is unlawfully used in the United States. The European position in these negotiations is likely to benefit from the fact that the U.S. public has become increasingly sensitized to data protection issues. Perceived deficits in personal data protection and criticism of the surveillance practices of U.S. intelligence services are becoming increasingly salient politically. Voices across the political spectrum[97] and in recent decisions of lower-level courts[98] have expressed doubt whether the collection of data on the gigantic scale practiced by the NSA is necessary to the counter-terrorism effort. Attention has been drawn also to the fact that the penetration by intelligence agencies of data managed by U.S. high-tech firms threatens their reputation and could later have massive economic consequences.

Transnational Conflicts

The conflict between the United States and the EU on issues of personal data protection is politically explosive because it directly affects the relationship between governments and citizens. Privacy may well be an issue in international relations, but above all, it is an issue of domestic politics and is a constitutive element of the design of public order. The transatlantic partnership will remain stable in the long run only if it is anchored in social mores. But this anchorage is slipping because the cyber security policies of the United States and the EU stand in growing opposition to central civil rights, to matters of personal privacy, and to the free use of content on the Internet. Currently, these conflicts represent in all likelihood the gravest long-term threat to the transatlantic cyber partnership.

Civil Rights on the Defensive

NSA spying practices have stoked conflict not only between U.S. and European governments but also between these governments and their own citizens.[99] For all intents and purposes, a transatlantic intergovernmental precedent for the wholesale collection and analysis of personal communication data has been established, a precedent not compatible with basic civil rights and liberties.[100] Strikingly, the monitoring operations of the intelligence services NSA and Government Communications Headquarters have met with little serious protest from the European governments who have been targeted for surveillance or whose citizens are being spied on. The analysis software Xkeyscore is used not only by the NSA but also by the German foreign intelligence service *(Bundesnachrichtendienst)*. Further, Germany's domestic intelligence service *(BundesamtfürVerfassungsschutz)* reported that it had been provided with a trial version. In fact,

96 Viviane Reding, "Reform durchsetzen," *Handelsblatt*, October 13, 2013, 48.

97 Two House Republicans, Justin Amash and F. James Sensenbrenner, and Democratic Senator Ron Wyden were united in criticizing Congress's failure to check presidential power at a conference of the Cato Institute, "NSA Surveillance: What We Know; What to Do about It?" (Washington, DC, October 9,2013); commentaries by Jennifer Granick (Center for Internet and Society, Stanford Law School), http://cyberlaw.stanford.edu/about/people/jennifer-granick.

98 Ellen Nakashima and Ann E. Marimow, "Judge: NSA's Collecting of Phone Records is Probably Unconstitutional," *The Washington Post*, December 16, 2013.

99 Laura Poitras, Marcel Rosenbach, and Holger Stark, "Codename 'Apalachee': How America Spies on Europe and the UN," *Der Spiegel*, no. 35 (26 August 2013): 85–89; Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *The New York Times*, September 5, 2013.

100 Stefan Heumann and Ben Scott, *Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany* (Berlin: Stiftung Neue Verantwortung, September 2013); KleineAnfrage der Abgeordneten Dr. Konstantin von Notz et al., "Geheime Kooperationsprojekte zwischen deutschen und U.S.-Geheimdiensten" (Berlin: Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/14759, September 16, 2013).

the federal government even defended U.S. practices with the argument that the NSA is undertaking "a clearly targeted collection of the communications of suspects in the areas of organized crime and the proliferation of weapons of mass destruction for the purpose of protecting the national security of the United States."[101] Through the summer of 2013, at least, the government was still basing its position on information provided by U.S. authorities. The government also stated then that German citizens were not being monitored on a massive scale.[102]

The privatization of knowledge extracted from mass data is now under critical observation on both sides of the Atlantic. The once pervasive Western myth that the Internet is a sealed-off virtual world of greater privacy and independence from social and political institutions[103] is being increasingly belied by the facts. In a world of cross-border communication flows, citizens are but weakly protected by constitutional rights or by legal frameworks — for the regulation of data retention, for example — embedded on the national or EU levels. Within the EU, the biggest problem is that EU countries use retained data not only to combat terrorism and international crime. Under the E-Privacy Directive,[104] such data may also be used for other purposes that need not be clearly defined and thus could include crime prevention or the maintenance of public order.[105] The most important transatlantic legal documents for fighting crime (the Budapest Convention) and for transferring international law to cyber warfare (Tallinn Manual) show little sensitivity for citizens' rights.

The Budapest Convention is highly controversial among human rights activists and privacy advocates. Article 16 of the convention stipulates that service providers must retain stored computer data for 90 days so that prosecuting authorities in criminal cases can gain access to these data under conventional law enforcement and legal aid treaties. The duration of storage can be extended on the request of one party. The convention also makes it possible for signatory states to provide real-time monitoring of traffic and connection data and even content. Service providers must also provide law enforcement authorities with customers' personal information at the behest of those authorities, even if the person is only a preliminary suspect. Companies operating in the United States must allow U.S. authorities access to data stored in Europe. Any information that an intelligence service is barred from collecting in its own country is collected and shared by an affiliated intelligence service.

The Tallinn Manual, too, has come under fire in this context. The broad definition of a military attack does not in principle ban governments from taking military action against non-state groups or even individual alleged hackers. The U.S. Department of Defense broadened its authority and ability to combat attacks directed not only against its own systems, but also against private computers, including infrastructure abroad. Through this avenue, it is feared, warfare can become increasingly denationalized and the boundaries between police and military operations even more blurred. Given that the military is not required to respect due process or protect civil rights in its operations, there is a danger that the ethics of the drone war against terror could come to dominate cyber defense.

It is noteworthy that intergovernmental relations in the transatlantic cyber partnership are robust and healthy, but its ties to civil society are feeble. In cyber security and Internet governance, governing practices have started to become separated from the prerogatives of civil rights protection. A prime example is the diametrically opposed views of government officials and civil rights activists about how Edward Snowden's actions should be treated under the law.[106] Whenever a government reacts to newly perceived security

101 Note the opposing positions taken by the parties out of government: Anträge der Fraktionen von SPD (17/14677), Die Linke (17/14679) und Bündnis 90/Die Grünen (17/14676), in *heute im bundestag* (hib), (September 3, 2013) 444.

102 Antwort der Bundesregierung auf die KleineAnfrage der Abgeordneten Andrej Hunko u.a., "WeltweiteAusforschung der Telekommunikation über das U.S.-Programm PRISM," (Berlin: Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/14602, August 22, 2013).

103 Eric Schmidt and Jared Cohen, *Die Vernetzung der Welt* (Reinbek, 2013).

104 "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection law", *Official Journal of the European Union*, L 337, December 18, 2009; "Corrigendum to Directive 2009/136/EG," *Official Journal of the European Union*, L 241, September 10, 2013.

105 "Im Gespräch: EU-Innenkommissarin Cecilia Malmström," *Frankfurter AllgemeineZeitung*, July 4, 2013.

106 Nikolaj Nielsen, "Snowden to EU: Whistleblowers Need Protection," *EUobserver*, October 1, 2013.

threats by arrogating to itself new powers, it inevitably creates new threats to civil society.[107] It is therefore not surprising that civil society organizations have already brought suit against government policy in the European Court of Human Rights. Three of the most respected British civil society organizations (Big Brother Watch, Open Rights Group, and the English PEN) have filed a lawsuit against Great Britain, claiming that the wiretapping practices of GCHQ are contrary to Article 8 of the European Convention on Human Rights. They argue that the wholesale collection of British citizens' communications data, including persons not suspected of doing anything wrong, violates privacy protections.[108] In the United States, too, several lawsuits against NSA surveillance practices are still pending.

Human Security on the Defensive

Defense industry firms are increasingly turning out new products in the field of cyber security in the attempt to compensate for profit losses incurred because of cutbacks in weapons contracts.[109] They secure networks, build firewalls, and simulate hacker attacks. Sales in cyber security are currently growing by 10 percent annually.[110] Defense firms have bought several specialized technology companies, acquiring their software expertise. The U.S. company Raytheon has acquired 11 IT firms since 2007, most recently Teligy, a company that specializes in wireless communication.[111] The defense company Cassidian is planning to increase the number of its cyber experts to 700 in the coming years. Defense firms traditionally were shielded from market competition, but they now compete with civilian companies such as Intel and Dell in the markets for IT security. This expansion of defense firms into the IT branch will serve to blur the boundaries between civilian and military enterprises, a trend that is well illustrated by the British defense contractor BAE's plans to cooperate with the mobile communications company Vodafone.[112]

The human rights organization Privacy International lists around 160 companies whose software products can also be used to monitor or suppress dissidents.[113] A majority of the companies are based in Europe or the United States. Through the export of their software, they help authoritarian governments suppress free speech and violate human rights. Their actions hinder the spread of democracy and undermine long-term global political stability. Companies that put insecure software on the market likewise facilitate the surveillance activities of authoritarian states.[114] Cyber security technology can raise the same kinds of ethical issues as traditional weapons technology. The Munich-based firm Gamma International is a good example. It sells a malware product of its own development, FinFisher, that can spy on computers and eavesdrop on mobile phone conversations. Working with partners, the company sells the program worldwide to police agencies and intelligence services. Human rights activists accuse Gamma International of selling to dictators. The company has responded that it consults the export control lists of Germany, Great Britain, and the United States before each sale.[115] Gamma International is not the only company under criticism. The Swedish telecommunications company TeliaSonera has exported its products to the successor states of the Soviet Union, and the U.S. network equipment company BlueCoat has provided surveillance technology to countries such as Iran, Syria, Sudan, North Korea, and Cuba, which are subject to U.S. sanctions, or to countries that have committed massive human rights violations and have

107 "Wenn die Macht schweigt. Ilija Trojanow, Juli Zeh und der Geheimdienst im Netz," in *Süddeutsche Zeitung*, October 4, 2013, 11; John Lanchester, "The Snowden Files: Why the British Public Should Be Worried about GCHQ," *The Guardian*, October 3, 2013; Ken Auletta, "Freedom of Information. A British Newspaper Wants to Take Its Aggressive Investigations Global, but Money Is Running Out," *The New Yorker*, October 7, 2013.

108 Constanze Kurz, "Die Menschenrechte sollen es richten," *FrankfurterAllgemeineZeitung*, October 4, 2013, 38.

109 Stockholm International Peace Research Institute (SIPRI), *SIPRI Yearbook 2013* (Stockholm et al., 2013), Chapter 3 (Military Expenditure), Point I (Global Developments in Military Expenditure).

110 PricewaterhouseCoopers, *Cyber Security M & A. Decoding Deals in the Global Cyber Security Industry* (November 2011), 5.

111 Ryan Gallagher, "Software that Tracks People on Social Media Created by Defence Firm," *The Guardian*, February 10, 2013.

112 "A Strategic Partnership with Vodafone," *BAESystems*, February 17, 2013.

113 Privacy International, "Global Surveillance Monitor," https://www.privacyinternational.org/projects/global-surveillance-monitor; Wall Street Journal, "Surveillance Catalog", http://projects.wsj.com/surveillance-catalog/#/.

114 "Russland plant die totale Überwachung im Internet,"*Deutsche Wirtschafts-Nachrichten*, October 21, 2013.

115 Hanna Lütke-Lanfer, "Ein Trojaner für den König," *Die Zeit*, February 14, 2013.

suppressed opposition groups, such as Egypt, Bahrain, Kuwait, and Saudi Arabia.

Critics are therefore of the opinion that export controls for sensitive software should be reformed so as to hold exporting companies and the export control regimes of EU member states to a higher standard of accountability.[116] The Electronic Frontier Foundation, Citizen Lab, and Privacy International have put forward important proposals for improving controls. They suggest that businesses be allowed to export critical software only to countries that protect human rights or that at least allow opposition groups unhindered freedom of expression. Under this proposal, the protection of human rights would be made a prerequisite for receiving a temporary license that would have to be rescinded should human rights violations occur after purchase. Another suggestion is to label software with the exact conditions under which it may be used. In this way, businesses could be required to prove that the use of their software is tied to specific conditions. In addition, some surveillance tools like Trojans could be classified as weapons and thus made subject to stricter authorization regulations.

Current export controls are ill-fitted to digital technology and need to be adapted to the Internet age.[117] The Obama administration issued an executive order in April 2012 to prevent the export of information and communication technology to Iran and Syria. It also placed export controls on software that enables surreptitious listening. The EU, too, imposed an embargo on Syria and currently prohibits the export of "dual-use" goods (products, technologies, and knowledge that can serve both civilian and military purposes) to countries under arms embargo, but it currently does not systematically check the human rights situation in technology-purchasing countries. The EP announced in September 2011 that it favors tighter regulation of surveillance technology exports, especially of dual-use goods. Individual states such as the Netherlands and Denmark have proposed making the granting of export permits for sensitive goods dependent on a stricter, mandatory review of human rights and democracy in receiving countries. In a response from October 2011 to the Green Paper of the European Commission on the dual-use control system of the European Union, the German federal government expressly demanded that in the future, balanced consideration should be given to foreign and security policy issues as well as business interests.[118] EU member states want to implement effective measures to adapt control mechanisms to political and technical developments, but they want to do it primarily at the international level.[119] The German federal government is taking part in related negotiations within the framework of the Wassenaar Arrangement.[120]

116 Wolfgang Ischinger, "Mehr Macht dem Parlament," *Handelsblatt*, August 30, 2012: 56.

117 Danielle Kehl and Tim Maurer, *Against Hypocrisy: Updating Export Controls for the Digital Age* (Washington, DC/New York: New America Foundation, March 9, 2013).

Freedom of Use versus Copyright Protection

Critics fear that Internet freedoms are increasingly being subordinated to the logic of product commercialization in markets. Symptomatic of this debate were disputes, lasting until 2012, over the Anti-Counterfeiting Trade Agreement (ACTA), a saga that began in 2007 when the EU and the United States announced[121] their intention to organize international cooperation against product piracy and counterfeiting in conjunction with countries such as Japan, Canada, Korea, Mexico, Morocco, New Zealand, and Switzerland. A trade agreement was sought that makes the commercial exploitation of intellectual property more secure and that protects consumers against the health and safety hazards associated with counterfeit products. When this original objective was then expanded to encompass the Internet and copyright infringement, ACTA became noticeably more political. The agreement that emerged provided for some quite severe penalties, even the blockage of Internet accounts. For many protesters, the contract is symbolic of the greater problem that a mere extension of the "intellectual

118 Antwort der Bundesregierung auf die KleineAnfrage der Abgeordneten Dr. Konstantin von Notz u.a., "Haltung der Bundesregierung bezüglich des Exports von 'Dual-use-Gütern' im Bereich der Technologie zur Störung von Telekommunikationsdiensten sowie Techniken zur Überwachung und Unterbrechung des Internetverkehrs durch deutsche Firmen" (Berlin: Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/8052, December 2, 2011): 2.

119 U.S. Department of Commerce, Bureau of Industry and Security, *2013 Report on Foreign Policy-based Export Control* (Washington, DC, 2013).

120 http://www.wassenaar.org. Guido Westerwelle, Ewa Björling, Laurent Fabius, and William Hague, "So muss der Waffenhandel global reguliert werden," *Financial Times Deutschland*, July 2, 2012: 24.

121 Stefan Krempl, "EU und United States treiben Abkommen gegen Produktpiraterie voran," *heise.de*, October 24, 2007.

property" system prevents the adaptation of copyright law to the needs of the digital society. As protests grew, the European Parliament announced its opposition to the agreement in July 2012. For most observers, this spelled the end of an initiative championed by leading industrial nations and worked out largely behind closed doors.[122]

In current debates on the Trans-Pacific Partnership (TPP) and the Trans-Atlantic Trade and Investment Partnership (TTIP), many of the same critiques of the ACTA reappear.[123] The TTIP is intended to tighten transatlantic protections in patent or copyright law and will probably include a dispute settlement procedure by which corporations could bring suit against nation states over regulations that are harmful to their interests. The settlement procedure exists already: Investor-State Dispute Settlement (ISDS) was originally created to protect investors from arbitrary government regulations and court decisions in countries with inadequate legal protections. The procedure has come to be used mainly by U.S. corporations. Parties not involved in the dispute are not granted access to the adjudication proceedings; typically, the U.S. parties involved voluntarily grant industrial associations complete access to the process while withholding information from other interested actors. Decisions may not be appealed. The "Seattle to Brussels" network warns in a report entitled "A Brave New Transatlantic Partnership" that the new trade agreement could revive the "spirit of ACTA" by expanding the number of cases heard under ISDS.[124]

The Foundation for a Free Information Infrastructure (FFII) also rejects the ISDS procedure[125] because companies could use it to weaken user rights in copyright law or to block "fair use" provisions currently under discussion. In U.S. copyright law, the "fair use" clause generally allows forms of use that do not threaten conventional value chains. Article 5 of the EU Copyright Directive (InfoSoc Directive), in contrast, grants exceptions from copyright protection only in enumerated instances. Copyright regulations are therefore more restrictive in Europe. The European approach so far has been less a problem for end-users than for innovative companies. Most copyright collectives are smart enough not to seek prosecution of individuals who infringe on copyright law but rather bring suit against companies whose services make such infringements possible in one way or another. For this reason, a greater number of innovative services arise in the United States than in Europe.[126]

122 Stefan Krempl, "EU Parlament beerdigt ACTA," *heise.de*, July 4, 2012.

123 Stefan Krempl, "Transatlantisches Freihandelsabkommen: 'Schlimmer als ACTA'," *heise.de*, October 11, 2013.

124 Kim Bizzarri, *A Brave New Transatlantic Partnership* (Brussels: Seattle to Brussels Network, October 2013), http://www.s2bnetwork.org/fileadmin/dateien/downloads/Brave_New_Atlantic_ Partnership.pdf.

125 "FFII Condemns Investor-to-state Arbitration in Trade Talks with U.S.," *FFII Acta Blog*, June 14, 2013.

126 Leonhard Dobusch, "Urheberrecht: Standortfaktor für digitale Innovationsoffenheit," in *Kompendium Digitale Standortpolitik*, ed.Baums and Scott (see note 12): 116f.

Recommendations for Transatlantic Cooperation

The transatlantic cyber partnership stands on a firm foundation of common principles and institutions, but it does not stand above the eroding effects of political controversy. The partnership is currently being tested. Its long-term stability requires that both sides overcome a number of serious differences.

1. In the continuing debates over cyber security, Internet governance, data protection, and surveillance of allies, it is important for both sides to recognize each other as equal partners. This means that the United States must give up its anachronistic attempts at unilaterally setting the rules of appropriate state behavior in international relations. At the same time, Europeans must develop a common position on all the relevant issues and engage the United States with one voice. This holds true today and will continue to hold true for years to come. In the medium term, it will be necessary for select NATO countries including the United States to commit to "no-spy" agreements with one another. Meanwhile, European states must endeavor to prevent the gap between insider and outsider states from widening. The emergence of a two-class society of informed and uninformed EU member states would be immensely harmful to the European project of integration.
2. Lost trust must be rebuilt among allied democracies. The disclosure of the NSA's transatlantic spying practices has deeply disrupted mutual confidence among the governments involved in the "wider transatlantic partnership." This is seen, for example, in Brazil and Germany's initiative to amend the International Covenant on Civil and Political Rights with provisions eschewing espionage of cosignatory governments. It is certainly remarkable that two of the United States' most important allies consider it necessary to adjust international legal standards in order to keep their friend under better control. The significance of this action cannot be overestimated, for it represents nothing less than a deep crisis of confidence in the transatlantic partnership. Both sides need to be aware that the idea of a free and open Internet can be realized only if there is consensus not only on how the Internet should be governed but also on why transatlantic cooperation in Internet governance and cyber security is meaningful. All attempts of authoritarian states to gain greater state control of critical content must be rejected decisively. To this end, the United States, the EU, and other democratic nations must work especially closely, because only together will they be able to set global standards and preserve the openness and freedom of the Internet. Importantly, neither the United States nor Europe can achieve its governance objectives without the other.
3. The Internet has become vital for the continuing health and growth of more than one area of social intercourse and will certainly play a positive role in maintaining a sustainable public order in the future. This means that the transatlantic partnership must also be anchored transnationally if it is to be stable in the long term. Citizens on both sides of the Atlantic have become more acutely aware than ever before of the drawbacks to digitalization, and calls for a renationalization of communication structures are more noticeable. A major transparency initiative is now necessary to stave off this threatening development. It is essential to comprehensively inform the public about U.S. and European industrial and security data usage practices and to make clear why this public disclosure is necessary. Anything less would leave unchecked the current erosion of trust between governments and citizens, and losing this trust would mean losing a most precious asset for the maintenance of liberal democracy.
4. The realization must also set in that the three major issues of cyber security, Internet governance, and data protection are a single policy package. Too often, the three topics are treated independently of each other, without insight into the complexity of their interaction. Further, cyber security will be elusive as long as important countries like Turkey, Brazil, India, and South Africa are not included in Internet governance and its analysis. The same applies to countries like Russia and China, whose inclusion is more difficult to achieve but imperative nonetheless. Finally, both sides might realize that deterrence alone does not create security, nor

will narrowly focused reforms of data protection law by themselves make for a comprehensive data usage policy. It is extremely important to understand that the state plays a different role in each of the three areas of Internet governance, cyber security, and data protection. The globalized world is based on cross-border digitization of infrastructure, of value chains, and of life worlds. In the future, for reasons of security, states must play a more active role in the protection of critical infrastructure than they have played in the economic and technical development of value chains. For the time being, private actors and others involved in autonomous multistakeholder coordination should step up and do their work. For the regulation of interaction in social networks and in the social environment generally, however, we should insist that state intervention is acceptable only under very narrowly defined conditions.

5. The fact that the three major issues of cyber security, Internet governance, and data protection are intimately connected should have consequences for the openness to consultation at the highest administrative levels. Reciprocal consultation must take place among the various responsible Directorates General of the European Commission and the General Secretariat of the Council of the European Union and among the relevant subordinate departments of interior, defense, economic, and justice ministries on both sides of the Atlantic. The United States already has a cyber coordinator, a position created in 2009 at the State Department. The EU has yet to take such a step. It is also imperative that the transatlantic dialog among legislators on matters of cyber security, Internet governance, data protection, and data use be intensified and expanded to include civil society actors. Policymakers in cyber security, Internet governance, and data policy should take account of concerns brought up by civil society activists and by the scientific community in every step of the coordination process. Only then can a long-term transatlantic cyber partnership come to rest on a firm foundation of values shared by governments across the Atlantic and by governments and citizens transnationally.

Abbreviations

ACTA	Anti-Counterfeiting Trade Agreement
BDI	Bundesverband der Deutschen Industrie
BRIC	Brazil, Russia, India, and China
BSI	BundesamtfürSicherheit in der Informations-technik (German Federal Office for Information Security)
CDC SC	Cyber Defence Coordination and Support Center
CDMB	Cyber Defence Management Board
CEN	ComitéEuropéen de Normalisation
CENELEC	ComitéEuropéen de Coordination des NormesÉlectriques
CERTs	Computer Emergency Response Teams
CIA	Central Intelligence Agency (United States)
CSBMs	Confidence and Security Building Measures
CSCG	Cyber Security Coordination Group
CSIS	Center for Strategic and International Studies (Washington, DC)
DPPC	Defence Policy and Planning Committee
EC3	European Cybercrime Centre
EFTA	European Free Trade Association
ENISA	European Network and Information Security Agency
EP	European Parliament
EP3R	European Public-Private Partnership for Resilience
ETSI	European Telecommunications Standards Institute
EU	European Union
EUISS	European Union Institute for Security Studies (Paris)
FCC	Federal Communications Commission (United States)
FISA	Foreign Intelligence Surveillance Act
FISAA	Foreign Intelligence Surveillance Amendments Act
G8	Group of Eight (the seven leading Western industrialized nations plus Russia)
GCHQ	Government Communications Headquarters (GB)
IBSA	India, Brazil, and South Africa Dialogue Forum
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
ISDS	Investor-State Dispute Settlement
ISOC	Internet Society
IT	Information Technology
ITR	International Telecommunication Regulations
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
NATO C3B	NATO Consultation, Command and Control Board
NCIRC	NATO Computer Incident Response Capability
NIS	Net and Information Security
NRO	National Reconnaissance Office (United States)
NSA	National Security Agency (United States)
OECD	Organization for Economic Cooperation and Development
OSCE	Organization for Security and Cooperation in Europe
PEN	Poets, Essayists, Novelists
PNR	Passenger Name Record
SCS	Special Collection Service
TDL	Trust in Digital Life
TFTP	Terrorist Finance Tracking Program
TPP	Trans-Pacific Partnership
TTIP	Transatlantic Trade and Investment Partnership
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
UN	United Nations
WCIT	World Conference on International Telecommunications
WGIG	Working Group on Internet Governance
WSIS	World Summit on the Information Society