Open security. Contributions of networked approaches to the challenge of democratic Internet security governance.

Andreas Schmidt

Discussions on Internet security and the appropriate institutions to contain Internet-related risks and threats are filling the conference rooms and meeting tables of academics, policy makers, and cyber intellectuals. Policy makers and national bureaucracies have reacted to rising numbers of Internet security incidents and the perception of increased vulnerabilities. Over the past years, traditional security institutions such as military, intelligence and law enforcement have increased their attention on questions of Internet security. Every other week, another country updates its cybersecurity strategy, proposes new Internet security-related legislation, or sets up yet another cybersecurity initiative.

Ideas about appropriate designs for Internet security institutions are exchanged in countless policy forums. Yet little of the institutional and organisational innovations that have been facilitated by Internet-based technologies appear to spill over to the sphere of security policy. Official Internet security polity is designed along the trodden paths of public-private partnerships and national security provisioning by traditional security institutions. Discussions about new forms of distributed collaboration among private and public organisations are scarce in the domain of Internet security (Dunn-Cavelty & Suter 2009). Furthermore, research on those actors and their collaborative endeavours that have kept the Internet up and running after numerous security incidents has literally been absent. At the same time, recent revelations about secret security and surveillance measures stress the problem of designing an Internet security polity architecture that adheres to democratic standards.

This chapter aims at addressing the aforementioned shortcomings by discussing two types of networked governance: the prevalent form of public-private cooperation, public-private partnerships and the more distributed, bottom-up model of Internet security communities. The challenge in Internet security governance is to find an institutional architecture that provides security in an efficient way. At the same time it needs to prevent mission creep, provide sufficient checks against centralisation of authority, and facilitate sufficient degrees of transparency and accountability. This chapter argues that security communities can moderate some of the normative deficiencies of partnership-based forms of public-private cooperation.

This chapter is organised as follows. The next section discusses public-private partnerships as a currently prevailing organisational approach to Internet security governance. The

ensuing section then describes the so-called Internet security communities with their distributed bottom-up collaboration as an existing alternative to provide similar services as public-private partnerships (PPP). The final two sections then compare both approaches, elaborate on the normative value of peer-producing distributed networks in the domain of Internet security and ponder ways to increase their utility.

Public-private collaboration

PPP as panacea to the cybersecurity polity problem

The regulatory and polity challenge for Internet security has quite a simple cause. States, whose core feature according to liberal-conservative theory s to uphold order, provide public security and protect citizens from criminals and external aggressors, either own nor have direct control over the technical systems that make up the Internet. Private companies, which own these components, have economic interests that are not necessarily congruent with the public's need for security. Furthermore, states can have conflicting security interests, complicating attempts for transnational collaboration.

States have responded to these challenges by setting up public-private partnerships as the perceived "panacea for this problem" (Dunn-Cavelty & Suter 2009, p. 179) .The underlying idea of PPP as it was defined by scholars of New Public Management is that a partnership between legal entities from the private sector and public authorities is in some cases the most efficient way to achieve certain goals or public goods (ibid., p. 180) .In reality though, the term PPP is applied to such a wide range of modalities of public-private cooperation that "the majority of so-called PPP in CIP [critical infrastructure protection; A.S.] are not really PPP at all" (ibid., p. 181) and that "referring to a PPP is a euphemism which does not resolve the main challenge to identify and implement an effective governance framework" (Irion 2012, p. 13). Dunn-Cavelty and Suter aim at re-establishing a narrow concept of PPPs and posit that their defining feature is that they are project-based, not program-based, have measurable goals and outcomes, and are usually based on formal contracts among players with complementary intentions (2009, pp. 181-182). A desktop-research report by the European Network and Information Security Agency (ENISA, 2011) chooses the opposite direction and implicitly creates a wide conceptualisation of PPP.

Irrespective of what the best conceptualisation of PPP might be, the popularity of these partnerships among policy makers has obviously spilled over to the domain of Internet security. Both in Europe and the US it appears to be the preferred governance mechanism.

In Europe for example, the EU has followed the idea of the European PPP for Resilience (EP3R), a project started in 2009[1]. With costs of cybercrime apparently still rising, the European Commission considers its EP3R by now to be ineffective as it "has…no operational powers and… cannot intervene to fix NIS [network and information security;

[1] For a thorough analysis of EP3R, see Irion (2012).

AS] problems" and "has no formal standing and cannot require the private sector to report incidents" (2013a, p. 28). This critique on informal, non-enforceable information exchange under the EP3R regime has resulted in a European directive proposal that would mandate sharing of certain information and grant to-be established national "competent authorities" some authoritative control over attacked ICT systems (European Commission 2013b). The proposed EU-model would establish a new organisational security network, but one that differs from existing Internet security communities set up by technical experts. The NIS directive draft proposes a "cooperation network," in which the Commission and the planned national "competent authorities" share information on risks and actual attacks. A "cooperation network" will help to overcome some of the knowledge problems caused by insufficient sharing.

In the US, a number of legislative proposals have aimed at a similar direction, seeking to establish more formalised PPP models. Dating back to the Clinton administration, initial forms of private-public cooperation have been voluntary and focused on information sharing under the umbrella of *Information Sharing and Analysis Centers* (ISACs) (White House – National Security Council 1998). In the subsequent years and especially after the events in September 2001, an increasing number of private-public partnerships on all governmental levels were set up to enable a seamless flow of information to effectively respond to incidents (Nyswander Thomas, 2013, pp. 9-14). Apparently under the auspices of the *Critical Infrastructure Partnership Advisory Council* (CIPAC), councils for private players in critical sectors and their governmental counterparts were established, interconnected by a number of liaising councils.[2] Since 2008, collaboration in the defence sector has intensified. The *DIB* [Defence Industrial Base] *Collaborative Information Sharing Environment*, the *Joint Cybersecurity Services Pilot*, the *DIB Cyber Pilot* and the *Joint Cybersecurity Services Pilot* have created venues for reporting incidents and sharing information about ongoing attacks, risks and vulnerabilities. These projects included in various combinations civil and military bureaucracies within the Defence sector, defence contractors and their Internet Service Providers (Ibid., p. 24-25).

The most comprehensive for incident response is the *National Cybersecurity and Communications Integration Center* (NCCIC), which allows national authorities and the private sector to share information about ongoing or upcoming security issues and functions as the "national response center during a cyber or communications incident" (Ibid., p. 19). And finally, the National Cyber Forensics Training Alliance (NCFTA) brings together technical experts with law enforcement to facilitate national and international investigations in computer- and Internet-based crime.

---

[2] The CIPAC and its subgroup, the Cross-Sector Cyber Security Working Group (CSCSWG), facilitate cooperation mostly on policy development between *Sector Coordinating Councils* (SCC) and their governmental counterparts, *Government Coordinating Councils* (GCC). Some of the larger IT companies, which are also members of the IT sector's SCC, the *IT SCC*, have grouped together in the *Industry Consortium for Advancement of Security on the Internet* (ICASI) since 2008, establishing "a <forum of trust> in which industry leaders can work together." (Nyswander Thomas, 2013, p. 22)

Despite the breadth of cybersecurity PPPs in the US, a number of shortcomings remain: too few small and medium-sizes businesses take part in them; building trust continues to be a problem among a large number of participants; and the perspective of cybersecurity as a public good, not often shared in the private sector, appears to be a prerequisite for engaged participation (Nyswander Thomas, 2013, pp. 25-30). As a means to overcome these shortcomings, legislators have proposed new or supplementing organisational approaches and mandatory cooperation by private-sector organisations. Plans for a so-called National Information Sharing Organization (NISO) or a central "cybersecurity exchange" would create a centralised, national clearinghouse or exchange point for information sharing, incident response, and mutual assistance across all sectors in private businesses and government, supplementing or replacing existing PPPs; a "civic switchboard" would examine weaknesses in existing PPPs and foster collaboration among different PPPs (Ibid., pp. 40-46).

Critique of PPPs

Quite a few scholars of organisational aspects of Internet security are critical of PPPs to ameliorate the Internet security situation. Dan Assaf, Amitai Aviram, Kristina Irion, Myriam Dunn-Cavelty and Manuel Suter, have all highlighted the problems of applying the PPP model to the Internet security domain. In their view, the underlying goals of PPPs clash with those of any cybersecurity arrangement. PPPs strive for efficiency; they involve partners from the private sector, the ultimate economic interests of which do not necessarily overlap with the public's interest and can therefore impede the production of the public good cybersecurity.[3] Cybersecurity arrangements strive for security, which often implies inefficient precautions, secrecy, walled-gardens within and between participating organisations. Therefore, "the interests of the private industry and of the state in CIP are only partially convergent" (Dunn-Cavelty & Suter 2009, p. 182).

This convergence problem has raised doubts whether PPP is the best organisational approach to cybersecurity. Bauer and van Eeten (2009) argue that some of the misaligned incentives for owners of ICT infrastructure that contribute to the Internet security malaise

[3] Cybersecurity is often described as a public good or semi-public good. According to Assaf, cybersecurity is "not a pure public good," even though "it is non-rivalrous in consumption and it generates positive externalities." But "it is, at least to some extent, excludable." (Assaf 2007, p. 32) National security however is deemed a public good as it is " both non-excludable and non-rivalrous in consumption." (Ibid., p. 31) One could argue though that national security is a club good as it by definition excludes human beings living in other countries. Elke Krahmann reasonably differentiates between the different concepts of national security and their impact on the public-good-character of security: "If security is defined as the absence of threat, it appears to meet the criteria of a collective good. If security is defined in terms of deterrence, it seems to be a club good. Finally, if security is understood as the survival of a threat, it appears to be a private good. …Moreover, it is the understanding of security as the absence of threat that has led to the argument that peace, rather than national defence, is the archetypical collective good…." (Krahmann 2008, p. 386)

can be reversed by appropriate regulation, e.g. by delegation to a respective regulatory agency (similarly, Irion 2012, pp. 14-15). Irion sympathises with a "safe harbor style regulation,"[4] which would establish a system of enforced self-regulation at the EU level." (2012, p. 22) Furthermore, she proposes "open and transparent" deliberations on Internet security governance on the European level, accessibility for "all stakeholders" including civil society, co-regulation e.g. to set technical standards and benchmarks that are relevant for the safe harbor regulation. (Ibid., pp. 21-24) Analysing the US public-private partnership governance model for critical information infrastructure protection (CIIP), Dan Assaf concludes that public interest in security is not thoroughly aligned with business interest in profit maximization. His solution: a shift from self-regulation to enforced self-regulation. (Assaf 2009, p. 81) Introducing "explicit public accountability and oversight mechanisms" (Ibid., p. 76) would allow for an increased consulting of public interests in cybersecurity provisioning. Some of the elements of accountability Assaf mentions, such as a rationalised and professionalised bureaucracy, judicial review, and transparency (Ibid., p. 80), are apparently considered in Western capitals, as the description of policy debates in the previous section has shown.

In contrast, Dunn-Cavelty and Suter argue in favour of a more hands-off role for the state. An "expanded model," a "networked approach to governance" or "network governance" would be the more appropriate way to deal with the problem of how to secure critical infrastructures. Under the condition of high functional and technical specialisation, national bureaucracies would lack the knowledge to specify the required outcomes. The state therefore needs to acquire a different role in public-private cooperation and act as "coordinator and stimulator" of self-regulating networks. (Dunn-Cavelty & Suter 2009, p. 184) These networks could then make up for many of the deficiencies of PPPs.[5] For example, Dunn-Cavelty and Suter pick up Aviram's argument (2004, pp. 23-28) that pre-existing networks are better at enforcing norms than governmental bureaucracies that lack the technological skills to effectively monitor the performance of cutting-edge PPPs. (Dunn-Cavelty & Suter 2009, pp. 184-185) However, the first argument - that governmental bureaucracies lack the capabilities required for effective monitoring of PPP performance - is rendered invalid by the recent leaks on Western intelligence agencies, the US *National Security Agency* (NSA) and the UK *Government Communications Headquarters* (GCHQ). The leaks reveal substantial technological surveillance capacities of national intelligence agencies (see also Kuehn in this volume). Apart from that, the argument in favour of

[4] 'Safe harbor' style regulation is another approach to manipulate operators' incentive to contribute to and comply with private CIIP standard-setting in order to benefit from an exemption from a legislative default." (Irion 2012, p. 18)

[5] To some extent, Dunn-Cavelty and Suter replace one fuzzy concept with another one. Network governance can have many forms, ranging from Anne-Marie Slaughter's state- and bureaucracy-centric "networks of government officials" (Slaughter 2004, p. 1) to Michel Bauwens' concept of the "partner state" (Bauwens 2012), the purpose of which is to incubate general welfare-oriented P2P projects.

networks in order to increase cybersecurity is convincing.

Social production of Internet security

The existing literature both on the theory and empirics of the "networks approach," or networked governance, in the Internet security domain by and large ignores the different manifestations networks can have. The same holds true for policy discussions in the US, Europe, and other regions (e.g. on New Zealand: Shore et al 2011). Apparently, they fail to acknowledge both the theoretical possibility and practical existence of a different form of public-private cooperation in the Internet security domain—voluntary collaborative networks among individuals from both private and public organisations, delivering services akin to those of formal PPPs. From the perspective of traditional security governance, the idea of security provisioning by networks firms and public authorities is by itself still somewhat new. (Eilstrup-Sangiovanni 2007, pp. 10-19) The idea of security being provided by distributed global networks of technical experts is nothing but awkward and counter-intuitive for pundits of international relations. But it has both empirically happened (Schmidt 2012, Mueller 2013) and is theoretically feasible, and represents a stringent specialisation of the networked model.

When Powell introduced the idea of networks as an organisational supplement to firms and markets, trust was among their defining characteristics and the means which enabled transactions in networks. In ideal-type markets and hierarchies, it is money and authority that make things happen. Much of the literature deals with inter-organisational networks, i.e. networks in which firms or other types of organisations are the decisive nodes. An example that Powell gives are networks of manufacturers and their external suppliers in a vertical disintegrated car industry. (Powell 1990, p. 321) A network of geographically concentrated firms thus serves as an alternative to a vertically integrated firm. (Carney 1998, p. 457) The concept of trust though introduces a level of analysis problem, as the building of trust between organisations involves a strong inter-human element. Powell hypothesised that common "ethnic, geographic, ideological, or professional" characteristics would create a homogeneous group with mutual trust among "participants." (Powell 1990, p. 326) Nevertheless, the focus of the literature on business networks has generally been on firms.

A different, more prominent role of the individual in production networks became feasible with the emergence of online communities and Internet-based, distributed, self-organised, autonomous collaboration (see also chapter 1 in this volume). Most prominent examples of this type of peer production are open source software (OSS) projects like Linux or content production websites such as Wikipedia. In its ideal-type variant, open source software projects use an organisational approach that by and large eschews the organisational principles of authority and monetary incentives, which are are the sources of activities in hierarchies and markets. While this mode of production is probably applicable for the production of any intangible, informational good and service, the need for secrecy requires organisational precautions that result in a different, rather closed and exclusive form of

peer production. The following section elaborates on such Internet security communities that are based on individuals, their mutual deep interpersonal trust and intrinsic individual motivation.

The innovations in forms of production also affect the possibilities of public-private cooperation (PPC), of which PPPs are only a subset.[6] In practice, public-private cooperation can span phenomena as different as the Internet security community with its trust-based coordination mechanisms, co-financed PPP botnet mitigation centres, and the recently exposed secret surveillance programmes with the private sector as data provider and national intelligence agencies as sponsor and central data integrator and analyst. The reality of PPC allows international, egalitarian, flat, and open structures just as they encompass secretive contracts between governments and private service providers for the alleged purpose of national security. The theory of state-private cooperation and collaboration though lacks inclusion of flat, non-hierarchical networks. Dan Assaf (2008, pp. 6-7) has defined the "regulatory continuum" covering the forms in which critical information infrastructure protection (CIIP) could be provided, ranging from government ownership, to (enforced) self-regulation to market based provisioning. It is the mode of self-regulation, more specifically "self-organizing networks" (Dunn-Cavelty & Suter 2009, p. 180), which Dunn-Cavelty and Suter consider as the best organisational approach to CIIP. Apparently, the regulatory "continuum" from hierarchies to markets runs via networks. However, networks can take non-hierarchical and non-market forms that hardly fit into the center of Assaf's regulatory continuum, the two ends of which are demarcated by pure markets and pure hierarchies. To consider the full range of possible forms of public-private cooperation, all possible manifestations of networks require a distinct consideration. The following section looks into one particular form of networked provisioning of Internet security.

Internet security community

Response activities to Internet security incidents are not only driven by incident response PPP or Computer Emergency Response Teams (CERTs), but also by distinctive communities or ad-hoc groups, whose members are part of a wider security network. The Internet security community is a loosely coupled network of security experts who are organised and collaborate in partly temporary, partly permanent sub-communities. Just like the Internet is often dubbed as the network of networks, the Internet security community is the community of security communities. This section analyses some key characteristics such as access criteria, hierarchies, structures and boundaries within the overall community, and the motivations of its members to contribute. The findings of this section, which have partly been described in earlier articles, are based on a research project that has analysed technical response activities that followed large-scale security incidents. (Schmidt 2012;

[6] "PPP are only one of many possible forms of cooperation." (Dunn-Cavelty & Suter 2009, p. 185)

Mueller et al 2013; Schmidt 2013b; Schmidt 2013a)[7]

Communities

The Internet security community is a network of individuals, organisations, groups, and communities working on different aspects of Internet security. There is no hard and clear definition for *Internet security community*, though. The term itself is commonly used by those who take part in these communities. Individual communities are organised around a variety of criteria such as technologies, Internet services, temporary security issues, professional specialisation, or the sector of an individual member's affiliation.

Most prominent among the Internet security communities is presumably the CERT communities, the ideational umbrella of all *Computer Emergency Response Teams* or *Computer Security Incident Response Teams* (CSIRTs). CSIRTs function as operational teams that support individuals and organisations to adequately respond to a security attack.[8] Such CSIRTs are set up and maintained by large corporations, or political bodies willing to consolidate responses to security incidents, to establish support centres for affected organisations or, in the case of corporate CSIRTs, organisational units. Different CSIRTs cover different organisations, sectors, regions, and countries. Their communicational cultures differ widely. While academic CSIRTs are accessible and communicative, staffs of military CSIRTs are usually rather tight-lipped. Many CSIRTs are publicly funded organisations, or teams therein. From an organisational perspective, the CERT complex is a mixed bag of everything. Military CERTs certainly are governmental hierarchies. Other CERTs like the Dutch govcert.nl or the Estonian CERT.EE are teams within national authorities and serve as facilitators of more or less informal public-private cooperation. The *Forum of Incident Response and Security Teams* (FIRST) serves as an umbrella for all CERT activities worldwide and provides Internet security experts from around the world with opportunities for meet-ups and trust-building to foster collaboration under or outside the FIRST umbrella. TERENA's[9] incident response task-force, TF-CSIRT, is an umbrella for European CERTs with again a focus on trust-building to foster voluntary information exchange and collaboration among the participants. It has helped to create an informal collaborative network between CERTs in Europe. While the term CERT gives the impression of similarity among these institutions, there are respectable differences with regard to accountability, secretiveness, geographical focus, political control, and their utility for national political agenda. CERTs usually have some kind of organisational structure and are either formal legal entities or teams within one. But they have also formed

[7] One caveat though: my research project has not aimed at mapping the entire landscape of Internet security communities. The description of existing communities and their characteristics are therefore probably cursory and incomplete. Future research will hopefully complete the picture.

[8] CERT is a registered trademark of the *CERT Coordination Center* (CERT/CC) of Carnegie Mellon University. But generally, both terms are used synonymously. CERT/CC was established in 1988.

[9] TERENA is the acronym of the *Trans-European Research And Education Networking Association*, the European umbrella organisation of national academic and research networking providers.

informal communities for collaboration and information exchange between CERTs.

The so-called operational security communities represent a fascinating new organisational phenomenon of security production and form the core of the Internet security community. CERTs, visible and popular as they may be, usually do not have the capabilities, capacities, let alone the authority to implement technical measures required to cope with an ongoing attack. Attacks are discovered and mitigated at the screens of network and system administrators, security analysts and other technical personnel. This is where operational security communities step in. These communities facilitate cooperation among operational staff to mitigate or solve ongoing attacks, incidents on the Internet. Several communities have emerged, often dedicated to distinct operational aspects of the Internet such as the resolution of domain names, traffic routing, or Internet root services. Partly, existing informal communities have taken up security related tasks when the security situation of the Internet started deteriorating in the early 2000s. Partly, entirely new communities with a focus on security issues were created. As a response to the achievements and weaknesses of the response to a series of larger and sophisticated botnets, an influential operational community was established in 2010 under the umbrella of an Internet non-profit organisation that had been active in providing core Internet services for some twenty years. This operational community includes experts from a variety of fields of Internet security. They range from ISPs, content hosting providers, hardware and software vendors, financial institutions, DNS and email services, registrars, law enforcement organizations, CERT teams, and otherwise remarkable security expertise. This operational community arguably gathers Internet security expertise in a very comprehensive form.

These operational security communities by and large incorporate the same organisational principles that characterise many other technical communities. One unifying characteristic is that they have been established ad-hoc by technical experts who wanted to empower themselves to deal with ongoing security incidents. At a time when market solutions e.g. against botnets were not available and public authorities were particularly clueless, security experts had to join their forces to be able to quickly monitor, understand, and mitigate security situations. Malware has been of particular importance for adversary-launched attacks on ICT systems. Consequently, the response to almost any adversary-inflicted incident requires a thorough search and analysis of malware. Malware researchers from AV and security companies or academia exchange information, clues, intelligence, and botnet samples via a few mailing-list-based communities.

Recent developments suggest that the existing landscape of operational Internet security communities is being altered or at least supplemented by new variants of the networked approach. An example of such a newly formed network is the Cyber Security Forum Initiative (CSFI). CSFI is a the result of a private initiative, and incorporated as a US non-profit organisation. The Forum, which appears to have close links to US military, aims at educating the US military on cyber warfare and facilitating collaboration and information

sharing inside government, military, law-enforcement and industry.[10] While it is a "volunteer group" (Klimburg 2011) just like the Conficker Working Group, it differs from the widespread type of mailing-list-based Internet security groups in important aspects. Different from these mailings-list-based communities, thorough vetting is no prerequisite for basic membership at the CSFI, but some specific projects require US citizenship and security clearance. Active contribution is not a requirement to remain part of the group. This approach has allowed the CSFI to gather some "5000 Cyber Security and Cyber Warfare professionals" (ibid.), which are inconceivable for traditional operational-security groups, managed via the social network LinkedIn. Apparently, CSFI cooperates with US military organisations, as frequent postings for jobs that require US clearances and are related to US military indicate. CSFI also held joint recruitment sessions with the NATO Cooperative Cyber Defence Centre of Excellence,[11] and a dedicated "cyber-warfare division." This sort of community however is fundamentally different from traditional communities of technological experts with a role in operational Internet security.

Characteristics

Civil, bottom-up Internet security communities[12] have a number of characteristics that differ from other distributed forms of collaborative production of digital goods that have emerged with the rise of the Internet over the last two decades. Probably the most remarkable among them are global production endeavours that follow the principle of open source or peer production. This form of production has been defined as distributed collaboration among volunteers who contribute their time and work based on non-monetary, intrinsic motivation, resulting in goods that are freely shareable. (Benkler 2006) Some of these criteria can be found in security communities, too.

The goods and services of the security community are, other than those of the poster children of peer production, not directly consumable or usable goods such as a Linux distribution, a Wikipedia article, or a LibreOffice suite. These security-related services are created by and targeted at operational security professionals in organisations providing services or goods that are affected by Internet security incidents. The community has served as an organizer, facilitator, and coordinator of global incident response endeavours, thereby helping to re-establish the functionality of the Internet after significant incidents. (Schmidt 2012) Virtual response teams are formed *ad hoc* to deal with such incidents. Standing communities with various technical and organisations focuses serve as forums to relay sensitive information to affected and interested parties; they also serve as communication hubs for distributed, collaborative solving of technical and organisational problems. Those

---

[10] Cyber Security Forum Initiative. "About CSFI." Retrieved June 1, 2011, from http://www.csfi.us/?page=about.

[11] Cooperative Cyber Defence Centre of Excellence, 2011. "Recruiting Cyber Power Workshop." Retrieved August 2012 from http://www.ccdcoe.org/ICCC/CSFI_CCDCOE_Workshop.pdf

[12] Here, I focus on this more narrow conceptualisation of Internet security communities and ignore this more recent phenomenon of communities which perceive themselves as vigilantes for national Internet security rather that non-national Internet security and which closely cooperate with military cyber-units.

focuses span from malware analysis, backbone security, anti-phishing, anti-spam, or DNS security, to name but a few. Furthermore, information exchange within these standing communities enriches situational awareness about ongoing and arising threats, attacks, vulnerabilities, or incidents. Finally, the community ensures rapid collective assistance for those members that have become victims of an attack.

The communities are operated and organised by volunteers, just as the contributions and information shared with the communities are the result of voluntary efforts. Hence, they appear to be organised and coordinated neither by money nor by power, the two common coordinative mechanisms of markets and hierarchies. Individual motivations are akin to those that can be found in classic open source software communities, ranging from technological interest ('an itch to scratch'), the prospect of indirect appropriation, pleasure of creating solutions, to values. Hunting down the 'bad guys,' however, is a motivation that is presumably unique to these security communities.

Probably the most striking difference compared to popular peer production platforms is that security communities are access restricted and apply ex-ante quality assurance mechanisms. While access criteria vary among the communities, they tend to comprise one or more of the following: an operationally influential position, a proven track record on security issues, high degrees of professionalism, and being part of the personal web of trust of existing members. Furthermore, member are expected to adhere to community rules such as responsiveness towards requests of co-members (the so-called 'no lurkers'-rule), refraining from commercial appropriation of community services, and ensuring the confidentiality of shared information. Some open source communities have similar personnel selection mechanisms in place for roles that have the authority to decide which contributed code eventually goes into release builds of the software. (Dafermos 2012) The reason for such staff selection is that a "bad apple" with such roles could have a devastating effect on the products and services of the community. Quality control is not provided with "many eyes" to which "all bugs are shallow" as in open source projects, but by ensuring that only responsible, sensible, like-minded persons get delicate roles.

Once a person is proposed for membership, a vetting process is initiated, in which the aspirant is examined regarding the community's specific set of access criteria. For some groups, usually mailing lists, the responsibility lies with a single maintainer of the list. In most communities, however, candidates are vetted either by the group's board or in a joint effort by all community members. Some communities have recently introduced sophisticated tools for community-based initial peer vetting of aspirant and continuous rating of existing members.

A community member will usually only vouch for a new aspirant if a deep trust relationship between them already exists. The communities' glue is trust. A network operator cutting the Internet connection of one of his customers needs to have a great deal of trust in his community peer, who had asked for such a measure, despite working for a competing company. This deep trust is based on long-term collaboration and knowledge about the

technological savviness of the peer community member. It also requires a somewhat unusual relationship between employed community members and their employers. In the words of an interviewed community member: "The level of trust within the group is higher than with any employer of the people." Communities' policy usually is that no information is shared with third parties outside the community, which includes the employer, as long as the sharer hasn't explicitly consented to sharing with others. This model of split loyalty, or from the perspective of the employer, reduced loyalty, is known in open source software communities. To give an example, in OSS communities a community member might value the community's interest in clean software design and a lean set of features higher than his employer's interest in additional features; therefore the feature might not get implemented even if the developer is paid by the employer to contribute to this OSS project. (Benkler 2013, p. 224) While there are no actual figures about the percentage of community members who are incited by the employers to spend some of their working or professional time on security communities, it is probably safe to hypothesize that the majority of the employers profit from their employees' community membership in some way. The split-loyalty model however serves as a barrier against corporate and governmental aspirations to dominate a community's agenda, both in open source projects and in Internet security communities.

PPP vs. Internet security community

Reflecting on theoretical and practical differences of security provisioning networks is not purely an academic amusement. Different characteristics may yield different political consequences. This section therefore briefly compares PPPs with Internet security communities with regard to their normative value for Internet security governance. Two important characteristics from the perspective of democratic security governance are the distribution of authority and accountability.

There are some strong overlappings between PPPs and peer production communities in the Internet security domain. In a brief desktop research paper, ENISA has identified a wide range of characteristics for PPPs in the domain of network and information security. (ENISA 2011) The similarities between these organisational types are apparent, as Table 1 shows. They are unsurprising as both approaches are specialisations of networked governance. They seemingly differ in their evolution, as peer security communities are created and developed exclusively by bottom-up initiatives, membership is always voluntary, and Internet security communities hardly provide deterrence services.

Table 1: Characteristics of public-private partnerships, their manifestations in PPPs and in security communities[13]

Organisational	*Possible manifestations in PPPs*	*Manifestation in peer*

[13] Except for the rows below "Links," left and centre columns are compiled from ENISA 2((11.

criterion		*security communities*
Organisational structure	Run by one from within; run by a coordinating entity democratically peer led	All options
Roles and Responsibilities	Chair/secretariat/coordination by industry/gov't/mix	Chair provenance not relevant; no secretariat; peer-coordination
Duration type	Persistent community groups; working groups; rapid response groups	All options
Participation Type	Subscription; mandatory; voluntary	Voluntary
Interaction Type	Face-to-face meetings; virtual co-operation	Both
Membership rules	Accession; rights and responsibilities; exclusion	All options
Formal information usage agreements	NDAs; traffic light protocol; deed of confidentiality	NDAs; TLP
Scope	Deter; protect; detect; respond; recover	Usually all but deterrence
Services	Research/analysis; information exchange; rapid response; and 16 other services	Most of them
Threat types	natural hazards; system failure; cyber-crime; terrorism/nation state	Focus on system failure and cybercrime
Community coverage	Geographic; focus (sector; cross sector; thematic);	All options, but usually sector-independent
Evolution	Top down; bottom up; top down, grown bottom up	Presumably exclusively bottom up
Incentives	Cost savings; sharing a problem; privileged, scarce information; reputation	Similar for employers. Members: Diverse intrinsic motivations.
Links	Bi/trilateral (with mirror organisations in other countries); other PPPs; CERTs; regulator	Individuals as liaisons
Members	Organisations	Individuals
External authority	Persuasion; coercion if if legally granted	Persuasion only
Geographical focus	Predominantly (sub-)national; regional	Global/none; regional; national local
Accountability	Very limited	Very limited
Culture	Ditto. Also: focus on national assets, against adversarial countries	Geeky; technological; "one Internet"; against "bad guys"
Legal foundation	Legal entity or part of existing legal entity, usually based on formal agreement	usually virtual organisation

From the perspective of democratic governance, the key differences between both types of

networked governance lie in their membership, geographical reach, culture, and in particular their authority and accountability. First, members of PPPs are organisations from either private businesses or public authorities. In security communities, members are individuals. Consequently, the incentives for participation differ between these two organisational approaches. In PPPs, private organisations follow economic incentives or legislative coercion. In security communities, it is an individual security pundit who needs to be motivated to participate voluntarily or at least find an employer willing to fund an employee's time spent on security communities with an unclear return on investment. The second difference is a consequence of the first: The culture in security communities, which have been set up and are run by operational technical experts or technical security analysts, likely differs from the culture of those set up and chaired by corporate or public managers. The motivation of the members of PPP, public and private organisations, is to save costs, get better information, and help to protect member organisations or the cyber infrastructure of a nation. Opposed or at least supplemental to this is the community's interest in a functioning and working Internet on the global scale. The third fundamental difference is the geographical focus of the arrangements. PPPs tend to concentrate on national or at best regional affairs, e.g. the above-mentioned EP3R. But even if an organisation like FIRST aims at the global level, much of the relevant operational collaboration that has been initiated and fostered by meetings in the lobby of FIRST conferences still happens in peer security communities. Security communities on the other hand do not have a national or regional focus per se. However, as they are built on deep personal trust, which best grows with similar backgrounds and frequent interactions, the membership of security communities appear to mostly come from Western countries.

Fourth, PPPs arguably have a greater potential of authority than peer communities, both internally with regard to its members and externally towards non-members. Internal authority, i.e. the ability to influence the behaviour of its members, is influenced by a number of factors like members' incentives to participate in the first place, the type of participation and members, the organisational structure, and forms of confidentiality. This is not to say that distributed networks have no coercive capabilities, on the contrary. Aviram describes that *private legal systems* can be effective means to enforce certain behaviour among their members. (Aviram 2004, pp. 17-23) The calculus by members to adopt to certain rules or implement an unfavourable policy is that the overall net value of participation and community membership is deemed higher than the costs of implementation. Nevertheless, the portfolio of coercive means in a formal PPP with mandatory participation, high confidentiality, a monopoly of scarce, valuable information embedded in a national security culture is higher than in a voluntary bottom-up network of technical experts with individual motivations. External authority in both cases depends on the ability to persuade non-members. PPPs on the national or regional level can be granted direct (legal provisions) or indirect (a darker "shadow of hierarchy") coercive means by legislators, e.g. to create blacklists of unwanted Internet websites or bodies to set security

standards.

Fifth, probably one of the most decisive elements of democratic governance is the capacity to hold those making generally-binding rules accountable to the public. As Assaf has rightly stressed: “The choice of actor to whom an entity is accountable has consequences for the outcome to which that entity is accountable, and hence is quite substantial.” (Assaf 2009, p. 73) The substance and actual policies in a certain security governance regime, in which decision makers are accountable to the public, are different from those in a regime, in which decisions are only scrutinized by a handful of backbencher with non-disclosure agreements. Accountability, “the state of being answerable to someone” (Ibid.) with the potential to sanction unwanted behaviour, can come in various forms, usually categorized as *direct*, *exit*, *external* and *voice* modes of accountability. (Mueller 2009, pp. 94-97) Functioning as mechanisms to oversee corporations or PPPs, consumer choice could punish unwanted behaviour in transparent and diverse markets and lead to *exiting* existing relations. As *external* reviewers, “rationalised and professionalised bureaucracy [and] judicial review” (Assaf 2009, p. 80) can help to oversee the activities of market players and public authorities. Finally, transparency and voting are the nominal sovereign’s means to hold players in the security governance field accountable by raising their *voice* or *directly* removing them from their assignments. As to existing PPPs in the domain of CIIP, Assaf has already argued that existing “accountability mechanisms are insufficient for ensuring the public interest” and subsequently called for “additional public accountability mechanisms“ such as transparency and voting. (Ibid., pp. 76, 77)

At first sight, the accountability of the Internet security community is rather bleak from the public’s perspective. On the one hand, given the community’s non-transparency, there are no opportunities for the public to raise voice, let alone to take direct actions. Furthermore, the public cannot circumvent the activities of the communities, as the latter acts in total opaqueness. The information that is exchanged there, the actions that are taken—it all happens behind the scenes affecting unknown Internet-related services. Furthermore, the public has no direct external agent serving as the community’s reviewer. I don’t know of any community member coming from a traditional ICT civil society organisations. On the contrary, quite a few members of influential communities come from law enforcement organisations that have been exposed to occasionally serve as proxies for US intelligence agencies. On the other hand, the accountability of the community is not that bleak if it is viewed from the angle of its individual members. They can vote the chair of a community (though many of them likely have a meritocratic leadership); they can raise voice on the community’s mailing-lists or in real-world meetings; they also can exit the community and set up different ones. The latter however might become increasingly difficult as network externalities of each community rise in an arguably consolidating community landscape. All in all, one might argue that the members indirectly serve as the public’s imaginary external reviewer. This argument is supported by the diverse set of intrinsic motivations that make individual community members contribute their time and effort to Internet security issues.

Opening security

The Snowden leaks have exposed an almost sinister cooperation between states and internet companies, undermining individuals' privacy, their freedom of expression, technical integrity of communication and information systems to unilaterally foster national or hegemonic interests. The more important it thus is to contemplate about future paths of Internet security governance and ignore the state of Internet *realpolitik* for a moment.[14]

The Internet security community can be developed in different directions. Elsewhere (Schmidt 2013b), I argued that the community can be subtly altered by traditional powerful actors aiming to serve their monetary or power-related interests. But a different path for the community towards a non-national, global, user-serving, more accountable security provider is conceivable, too. First, the community needs to preserve its variety of mindsets. Its cultural diversity with persons coming from different backgrounds—national, professional, ideological, ideational—serves as a check-and-balance against its instrumentalization by traditional powerful actors. From the public's perspective, it is of importance that hacker-personalities remain part of the community to check those from or with close relations to traditional, overly secretive traditional security organisations.

Second, a profound goal should be its further globalisation. Currently, the community is predominantly composed of experts from the US, presumably followed by European countries. To create a true global institution that serves the global integrity of the Internet, these communities need to include a higher percentage of persons from other parts of the world. If states want to engage in some governance innovation as "partner states" (Bauwens 2012), they could sponsor communities at all geographical levels to regularly convene in a relaxed atmosphere, and create collaborative infrastructures.

Third, the public interest is arguably best served when collaboration is fostered by intrinsic motivations of its member rather than by political or direct economic interests of its membership. Therefore, the existing community model with individuals - not organisations - as members needs to be further strengthened.

Fourth, the community needs to avoid and combat any attempts by traditional powerful actors to hierarchize the community. Centralising the locus of authority and knowledge counter the federative, power-balancing structure of the community.

Fifth, the community should evaluate ways to become more transparent and open. A thorough analysis of levels of secrecy required for its internal informational goods might reveal opportunities to share more uncritical information and thereby build trust with the

[14] The sheer scale and scope of that secret surveillance and monitoring public-private partnership marginalises any previous debate on public-private partnership for critical information infrastructure protection or against cybercrime. This monitoring regime appears not to have been established by chance, by accident or only as a consequence to 9/11. There are strong indications that it is an implementation of a long-term foreign policy strategy which has its intellectual roots in the 1990s. (Schmidt, 2004) From that perspective, debating the future role of the Internet security community appears to be somewhat academic, indeed.

public. Granularly opening security data and creating true public spaces for non-members might also lead to security innovations. These suggestions certainly are only very rough ideas. After the Snowden leaks though, it is apparent that deep thinking needs to be invested into the design of global Internet security governance architecture.

Bibliography

Assaf, D., 2007. Government Intervention in Information Infrastructure Protection. *In:* E. Goetz & S. Shenoi (eds), *Critical Infrastructure Protection,* Boston: Springer, pp. 29-39.

Assaf, D., 2008. Models of critical information infrastructure protection. *International Journal of Critical Infrastructure Protection*. 1(0), pp. 6 - 14.

Assaf, D., 2009. Conceptualising the use of public-private partnerships as a regulatory arrangement in critical information infrastructure protection. *In:* A. Peters et al. (eds), *Non-State Actors as Standard Setters,* Cambridge: Cambridge University Press, pp. 61-83.

Aviram, A., 2004. Network Responses to Network Threats: The Evolution Into Private Cyber-Security Associations, *SSRN eLibrary*.

Bauer, J., and van Eeten, M., 2009. Cybersecurity: Stakeholder incentives, externalities, and policy options, *Telecommunications Policy*, 33(10-11), pp. 706-19.

Bauwens, V. 2012. Evolving towards a Partner State in an Ethical Economy. *In:* A. Botero, A. Gryf Paterson & J. Saad-Sulonen (eds), *Towards Peer Production In Public Services: Cases From Finland,* Helsinki: Aalto University, pp. 34-49.

Benkler, Y., 2006. *The Wealth of Networks: How Social Production Transforms Markets and Freedom.* New Haven, London: Yale University Press.

Benkler, Y., 2013. Practical Anarchism: Peer Mutualism, Market Power, and the Fallible State. *Politics & Society*, 41(2), pp. 213-51.

Carney, M., 1998. The Competitiveness of Networked Production: The Role of Trust and Asset Specificity, *Journal of Management Studies*, 35(4), pp. 457-79.

European Network and Information Security Agency, 2011. *Cooperative Models for Effective Public Private Partnerships—Desktop Research Report* [online] Available from: http://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps/desktop-reserach-on-public-private-partnership [Accessed 21 July 2013].

Dafermos, G., 2012. Authority In Peer Production: The Emergence Of Governance In The FreeBSD Project, *Journal of Peer Production* (1).

Dunn-Cavelty, M., & Suter, M., 2009. Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, 2(4), pp. 179-87.

European Commission, 2013a. Impact Assessment—Accompanying the document "Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union [online] Available from: http://www.statewatch.org/news/2013/feb/eu-com-network-info-security-swd-31-13.pdf [Accessed 1 May 2013].

European Commission, 2013b. Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. COM(2013) 48 final [online] Available from: http://www.eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf [1 May 2013].

Irion, K., 2012. *The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R).*

Klimburg, A., 2011. Mobilising Cyber Power, *Survival*, 53(1), pp. 41-60.

Krahmann, E., 2008. Security: Collective Good or Commodity? *European Journal of International Relations*, 14(3), pp. 379-404.

Mueller, M., 2009. ICANN Inc: Accountability and Participation in the Governance of Critical Internet Resources, *Korean Journal of Policy Studies*, 24(2), pp. 91-116.

Mueller, M., Schmidt, A. & Kuerbis, B., 2013. Internet Security and Networked Governance in International Relations. *International Studies Review,* 15, pp. 86-104.

Nyswander Thomas R., 2013. Securing Cyberspace Through Public-Private Partnership — A Comparative Analysis Of Partnership Models. Thesis [online] Available from: http://csis.org/files/publication/130819_tech_summary.pdf [Accessed 25 August 2013].

Powell, W.W., 1990, Neither Market nor Hierarchy: Network Forms of Organization, *Research in Organizational Behavior*, 12, pp. 295-336.

Schmidt A., 2004. Hegemonie durch Technologie — Strategien zur Instrumentalisierung von Informationstechnologien in globaler Politik – Überlegungen amerikanischer Think Tanks. Unpublished thesis.

Schmidt, A., 2012. At the boundaries of peer production: The organization of Internet security production in the cases of Estonia 2007 and Conficker, *Telecommunications Policy*, 36(6), pp. 451-61.

Schmidt, A., 2013a. The Estonian Cyberattacks. *In:* J. Healey (ed.), *The Fierce Domain – Conflicts in Cyberspace 1986-2012,* Washington, D.C: Atlantic Council.

Schmidt, A., 2013b (forthcoming). Hierarchies in networks—Emerging hybrids of networks and hierarchies for producing Internet security. *In:* J. Kremer & B. Müller (eds), *Cyber Space and International Relations—Theory, Prospects and Challenges (Working title).* New York: Springer.

Shore, M., Du, Y. & Zeadally, S., 2011. A Public-Private Partnership Model for National Cybersecurity, *Policy & Internet*, 3(2).

Slaughter, A.M., 2004. *A New World Order,* Princeton, NJ: Princeton University Press.

Eilstrup-Sangiovanni, M., 2007. *Varieties of Cooperation: Government Networks in International Security.* [online] Available from: http://cadmus.iue.it/dspace/handle/1814/7503 [Accessed 29 August 2013].

White House – National Security Council, 1998. *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* [online] Available from: http://clinton4.nara.gov/WH/EOP/NSC/html/documents/NSCDoc3.html [Accessed 29 August 2013].