Who Is to Safeguard Trust in Cyberspace?

Abstract

The world is becoming ever more digitised and networked, which is one of the manifold aspects of globalisation. Cyberspace penetrates at an impressive rate societies and societal practices, including the production of security. Digital infrastructure is or controls the backbone of contemporary Western societies. Even the production of national security depends on it, albeit majority of actors operating in the field of cyber security are not governmental but private companies. Security, again, is closely intertwined with trust. They reinforce one another. The alarming piece of news hence is that people increasingly do not trust the functions of digital infrastructure and that cyberspace can be secured. Traditionally, the production of security has been the main task of the state, but who should be responsible for safeguarding cyberspace? And, above all, whose responsibility it is to build and maintain trust in and on it?

Introduction

According to a poll conducted early this year in the United States “almost half of the respondents (47%) said they have changed their online behavior” after news about the National Security Agency’s activities. “Over one quarter of respondents (26%) said that, based on what they have learned about secret government surveillance, they are now doing less banking online and less online shopping.” Twenty-four per cent is less willing to even use email. The trend is not novel, but a strengthening one. (We Live Security 2.4.2014\(^1\)) In the autumn 2013 a similar study was conducted in Finland amongst business executives. Sixty-seven per cent of the executives were not surprised about the scope of surveillance. Only 10 per cent noted that the revelations had already affected their business operations and 51 per

---

\(^1\) The survey was conducted online within the United States by Harris Poll on behalf of ESET from February 4-6, 2014 among 2,034 U.S. adult adults ages 18 and older, among which 1,691 are at least somewhat familiar with the NSA revelations. This online survey is not based on a probability sample and therefore no estimate of theoretical sampling error can be calculated.
People are not concerned only about online privacy. According to a study conducted in the United Kingdom in early 2013 “consumers are now more aware of the potential threat posed by inadequate cyber security. When asked, 87 per cent of [them] claimed to have thought about being targeted by cyber criminals.” One in three consumers having experienced a security breach stopped dealing with the business in question, while 53 per cent said they were more likely to share their data online with a brand they trusted. Altogether, 88 per cent of respondents expected companies collecting their data to keep it secure. Yet some companies believed it was the consumers’ responsibility to protect their own data. (Deloitte 2013, 43.) In a comparative study on online authentication conducted in the US, the UK and Germany it was found that consumer trust in a website’s security may depend on the complexity of authentication. “In the US and UK less than half of respondents [46% and 45%] believe that trust is dependent upon the use of more than passwords for authentication purposes.” Sixty-five per cent of German consumers do not trust systems or websites with such authentication practices. (Ponemon Institute 2013, 6-74.)

These are only examples of studies pointing towards the same direction: people do not trust the digital world. Regardless of the evident trust issues, contemporary Western societies are highly dependent on functioning cyberspace. It would be difficult to imagine government, business, healthcare, transportation or any other everyday function to be carried out without it. In addition to the convenience that smart phones, tablets, laptops and computers bring into our lives, Western societies’ critical infrastructure runs on and/or is steered and controlled through cyberspace. Therefore, it is highly alarming that we do not trust the infrastructure that lays the ground for our daily lives. We recognise its importance, though, as the fact that securing cyberspace has become a question of national security production in the past years witnesses. Cyber security has risen onto agendas of all important multi- and bi-lateral meetings, negotiations and conferences. It has become a topic addressed in national and international political, military and economic fora alike.

In this article a definition of cyberspace as “the collection of computing devices connected by networks in which electronic information is stored and utilized, and communication takes place (Clark 2010, 1)” is accepted. Moreover, it is suggested that cyberspace “has a physical basis in hardware, yet software enables its operations. It includes all digital information created, as well as the users of this information.

---

2 The study was conducted by Nixu amongst business executives and CIOs of TOP-500 companies in Finland from August 28 to September 13, 2014. Information was gathered with a web-based questionnaire that was emailed to the target group, 904 persons in total. There were 86 responses received which is 9,5% of the target group.

3 The consumer survey was carried out by Ipsos Mori on behalf of Deloitte. It was conducted online with a nationally representative sample of over 2,000 UK adults aged 16 to 75 between 15-18 January 2013. Deloitte also conducted interviews with a number of leading consumer business executives on their attitudes to cyber security and experiences of cyber crime.

4 The sample response for the Ponemon study was conducted in November 2012. The consolidated sampling frame of consumers in all countries consisted of 47,625 individuals who were 18 years or older. From the sampling frame, 2,292 returns were captured of which 134 were rejected for reliability issues. Screening removed another 234 returns, resulting in a final sample of 1,924 or a 4 percent response rate.
Its physical basis and effects on global events intertwine cyberspace closely with the physical world.” (Salminen 2014, 84.) Cyberspace constitutes an important section of societies’ critical information infrastructure and both impacts and is affected by events in the physical world. When the society has been recognised as the primary object to be nationally secured, the importance of critical infrastructure protection has become highlighted.

Critical information infrastructure (CII) is a part of critical infrastructure (CI). The latter refers to structures and functions that keep the society running; which locate “under the society” and enable its smooth functioning. It consists of both physical and digital resources and structures. The former, again, consists of physical and virtual information systems which control, process, transmit or store digital content that steers CI or is in itself critical to the functions of the society. (Limnéll et al. 2014, 239.) According to Lewis (2006, vii) before 9/11 CI security was generally taken for granted as attacks against something potentially so devastating to the society were perceived unthinkable. This has led to a situation in which almost all CIs are vulnerable to attacks.

Protecting critical infrastructure is a constant battle taking place in equipment, computer networks and the human mind. As majority of CI is cyber-dependent, an important way of doing this is the practices of cyber security. According to Lewis (2006, 429) cyber security “is the study and practice of securing assets in cyber-space – the world of computer and computer networks”. In addition to defending against viruses and worms, it encompasses information assurance in enterprise computing (italics removed). Limnéll et al. define cyber security more broadly as balancing between opportunities and threats residing in cyberspace. It refers to the security of “the world of bits” which is closely intertwined with security in the physical world. It means a state of affairs which is characterised by trust induced by familiarity with and understanding of cyberspace, as well as the capability to foreshadow and hence control cyber threats through varying security measures. In addition, cyber security refers to the capability to resist threats and their effects. It is a dynamic concept that evolves constantly. (Limnéll et al. 2014, 15; 39; 42.)

When accepting Limnéll et al.’s definition as a starting point, it becomes evident that the networks meaningful to CI protection – and hence the well-being of the society – do not solely comprise computer networks. More extensively understood “[n]etwork is a set of interconnected nodes” that are of varying relevance to the network (Castells 2009, 19). The importance of a node arises from its ability to contribute to the effectiveness of the network in achieving its goals. The function and meaning of a node depend on how it interacts with other nodes and how the network is programmed. Networks operate on the logic of inclusion and exclusion. In general, they have the ability to reconfigure themselves, that is, to add new nodes and delete some old ones. (Castells 2009, 19-23.) “In social life, networks are communicative structures” that process information flows (Castells 2009, 20). Communication, again, refers to “the sharing of meaning through the exchange of information (Castells 2009, 54”).

In security production, according to Lewis, the central starting point should be the realisation that CI as a network entity is too vast and complex to be fully protected. Therefore, one needs to prioritise the nodes (or hubs) that are perceived most critical. (Lewis 2006, vii; 2.) Once the critical nodes are
protected, resilience built into the society will take care of the rest. Resilience, again, is highly dependent on trust that people feel towards one another and the societal structures. In a global network society in which the state is only one of the nodes, traditional security thinking does not work. Even if the production of security has been the prime task of the state and even if the state remains a pivotal security actor, it needs to create and become part of collaborative security structures in the emerging situation. Responsibility for protection needs to be (re-)distributed among a variety of actors who may not even know one another. What is needed is new kind of thinking that is based not on security of a territory and its inhabitants but of flows (of information) and critical network nodes. The ‘thing’ holding the structure together is trust. Its reinforcement is a task for a multiplicity of actors in their respective environments without any of them trying to attain control over the entity.

In this article, first, trust and security as well as the link between them are addressed. Then, the role of state in the provision of security and reinforcement of trust in the global network society is discussed. The necessity of extensive, cross-border collaboration in security production is acknowledged and, finally, a suggestive answer to the concern of expanding mistrust in cyberspace is given.

The link between trust and security

There are manifold descriptions of both trust and security. Neither of these discussions is addressed here in depth, but the point is to highlight their mutual relationship. There is relatively little literature on trust in an online environment (Connolly 2013, 263) whereas cyber security literature is predominantly technical in nature. Therefore, both trust and security are here defined as they are understood in the physical world while an assumption is made that the phenomena are not too different in the digital world. Nevertheless, it is acknowledged that engendering trust in cyberspace is more challenging than doing so in the physical world (Olson & Olson 2000).

Trust can be understood both as a direct relationship between two actors and a collective phenomenon. Its importance derives from its ability to facilitate interaction and serve as “means of reducing perceived risk in situations of uncertainty and complexity”. (Connolly 2013, 264; also Friedman et al. 2000, 34.) Trust is irrelevant in unambiguous environments, but becomes meaningful when imperfect knowledge exists and risk is present – as the situation in cyberspace is. It is a positive expectation about behavioural predictability and integrity – either in general or, more commonly, in a particular situation. It may be engendered or reinforced by institutional arrangements (like legislation, organisational rules or contracts), and it evolves over time hence being influenced by experience (one’s own or that of a third party, that is, through reputation). (Connolly 2013, 264-269.) Trusting is a vulnerable situation dependent on the benevolence of the trusted party and confidence of the one trusting. Its significance is highlighted in cyberspace where near anonymity prevails making it difficult to be sure that the other party even is who he or she claims to be. (Connolly 2013, 264-265; Friedman et al. 2000, 34.)

It is claimed that trust can only emerge between human beings. Why do we still speak about “trust in the system” or “trust in cyberspace”? According to Friedman et al. (2000, 35-36) we actually trust the designers of technology, not technology per se. Even if, for example, National Research Council’s (1999)
ground-laying report talks about trust when referring to systems that perform as expected, according to Friedman et al. (2000, 36) we need to differentiate between technical failures and breaches or breaks of trust. The former do not meet the criteria for seeking moral remedies as they are not moral questions, whereas trust-issues are. Moreover, it is sensible to talk about relying on technology, not trusting it. Not even if online systems actually create and depend on an environment which induces trust. According to Friedman et al. we can only trust the clues of trustworthiness that are drawn from the environment, not the environment per se. (Friedman et al. 2000, 36-37.)

In this article, it is believed that people show mainly mediated trust (or distrust) towards cyberspace while actually trusting the human element behind this artificial construct: the designer, manufacturer or seller of technology, societal remedies enforceable if trust is breached, insurance cover or people acting online. Nonetheless, because in their daily lives people do not differentiate between technology and those who built it and because polls and much of other data discuss particularly trust in technology, it is accepted as a variable. The question of why people do not differentiate between technology and its manufacturers is a topic for another study. However, the answer may lie somewhere along the lines that the meaning of technology in societies has changed. According to Airaksinen technology used to be for some purpose, that is, it was used for solving a problem, whereas today it solely exists. Technology is a crucial part of our everyday life, yet it has the sole function of being on or off. For this reason we do not even notice its existence; only when it does not function the way it is expected to. (Airaksinen 2003.)

How we relate to technology plays an important part in whether we trust it — and whether we perceive it safe and secure. Carr notes how in philosophy of technology there are three main approaches to technology. First of them perceives technology as a neutral, value-free means of addressing a problem defined by the human being. It justifies continuous innovation (turning what is technologically possible into reality). The second believes that technology is a kind of external force that influences society but over which society has little or no influence. It sees technology as imbued with values such as desire for power, quest for efficiency and profit motive — and deaf to changes in human values or desires to use technology in a particular way. The third sees technology as an expression of social, political and cultural values. Decisions about which technologies are developed and who benefits from them are formulated in societal power struggles and shaped by the cultural context. (Carr 2012, 173-176.) Different approaches to technology have prevailed in different periods of time; yet all of them exist and influence how trust and security in cyberspace are perceived and can be strengthened. This article leans most towards the third approach. There are additional approaches too, like for instance in Radu (2014).

Not only trust in technology is important, but trust through technology even more so. When trust in cyberspace is discussed from a technological perspective focus is usually on the latter. Trust is not seen as a moral question, but one of providing additional technical means of verification to induce trust. The

---

5 Radu (2014, 6) mentions three-pronged division in attitudes towards technology between “technical determinists, who have underscored technologies as the fundamental driver of society and cultural values”, “the sociotechnologic approach [which] has highlighted that the dynamics of technological change are potentiated by collective and individual choices and reflect underlying power relations”, and “the social constructivists, who have seen technology as socially constructed and entirely dependent on the interactions of individuals and groups and their ongoing (re)interpretation”.
lack of face-to-face experience and social cues are to be substituted by technology. For example, Friedman et al. think of trust as engineering question and conclude that “the goal should be to engineer technology that more suitably cultivates the conditions for trust online” (Friedman et al. 2000, 39). Usually, in this context discussion is about digital trust. There is no unanimous definition of the term, but basically it refers to technical solutions contributing to people’s confidence to act in cyberspace. For example, the means of digital identity authentication, legitimate credentials, strong encryption, privacy protection, digital signatures and time stamps, as well as electronic seals fall within this category. In some occasions, digital trust is also used as a term to describe trust in cyberspace in general. However, as trust in and through technology emphasise different aspects of online trust, it is beneficial to keep them separate. Moreover, trust, for instance, in e-commerce operates within a different framework than trust in critical infrastructure protection, e-voting, online game-worlds or communications between colleagues. Trust has somewhat different nuances in each of these settings, even if this article treats trust in cyberspace as a uniform concept.

Security, again, is both an objective state of affairs and a subjective perception in a situation. It can be seen as a preferred end-state which an actor strives for while different threats pose obstacles along the way. Most severe threats can even challenge the existence of the actor. Simply put (and defined in negative terms), security is a situation in which there are no threats in sight. Because such a situation does not exist in real life, security is always in coming, that is, a never ending process. There is no absolute security; especially in the digital world which is characterised by uncertainty and risk. As an artificial human creation cyberspace, in principle, is ever malleable. Truths of yesterday may no longer hold today which decreases predictability. In addition, and as it has often been noted, cyberspace was not designed and built security in mind. Instead, technological curiosity, convenience and usability drove the development. As cyberspace has become an integral part of our societies, there are claims made for re-engineering it so that security would be built into cyberspace. However, this is unlikely to take place because of inconvenience and cost.

Security is a concept which is defined variably in different contexts. It means a different thing in politics than in psychology, in information technology than in environmental studies. What is common to all conceptualisations, however, is that there always is an object to be secured, some threats to it and a need to find ways and means to counteract the threats (e.g. Williams 2008). In some instances, countermeasures are divided into defensive and offensive, yet to all contexts this division is not suitable. The state has historically been the focus of security analysis in political theory, especially in international affairs. It has been scrutinised both from within and in its relations to other states. Society, again, has been defined by the state borders, its administrative apparatus and nationalism (Castells 2009, 17). It has comprised both the state and the relatively free civil society operating within the state laid

---

6 Booth and Wheeler (2008, 134) note that uncertainty is “the ‘existential’ condition of human relations”, that is, “an everyday part of the existence of individuals and groups”. People can never be perfectly sure about the motives and intentions of others, yet life in any social setting is dependent on actions and reactions of others. The state of affairs leads into a situation named security dilemma which consists of a dilemma of interpretation (about the capabilities, intentions and motives of others) and a dilemma of response (about the most rational way of responding in the situation). (Booth & Wheeler 2008, 134-135; also Booth & Wheeler 2007.)
regulatory framework and borders (Berndtson 1995, 41). Security threats have primarily targeted the state; threats to society have been derivative from these.

Since the end of the Cold War the area which security covers has been both widened and deepened (e.g. C.A.S.E. Collective 2006). The conventional lines between, for instance, inside and outside (Walker 1993) as well as peace and war (e.g. Malkki 2008) have become blurred. In the past years, it has come to include cyber security as well; although, often as an attachment to traditional understanding of national security. The better acknowledgement of threats to society and human beings is important in relation to cyberspace because it has penetrated societies and societal practices first and further than it has pierced the administrative state. Security threats residing in cyberspace do not target primarily the state, but the different building blocks of society. The state, actually, may also pose a threat to some of these building blocks by exaggerating its security posture.

Alongside being characterised negatively as a lack of threats, security can be defined positively as a state of freedom – for instance, freedom of speech and worship, as well as freedom from fear and want. The first two are included in the list of basic human rights whereas the latter two are promoted especially by the United Nations within the Human Security framework. Human security concerns are generally addressed as questions of development with the aim of enhancing the stability of world order and hence the security of the Western states alike (Duffield 2007, 1-3). However, freedom of expression, right to privacy and fear related to excessive surveillance and the state’s unnecessary utilisation of emergency measures have kept bubbling on the surface of the state induced digital monitoring discussion for the past years (for example, Järvinen 2014; Clarke et al. 2014; Edwards 2014).

Widening and deepening of security have turned it into “a concept [that] saturates contemporary societies all around the world (Williams 2008, 1)”. The state of affairs has been referred to with a highly negative conceptualisation of “culture of fear” (Furedi 2002). This makes security a fluid concept which changes its meaning according to the context but is always present. It is political (inheriting obligatory choice and the related responsibility) and highly debated, because it enables the utilisation of emergency means (and the related resources) when perceived necessary. Thus, it is an important power resource. Being able to acceptably define an issue in terms of security grants an actor the right to do more or less everything needed for protection and safeguarding. (E.g. Wæver 1995.) However, security is not solely about survival. It is an enabler that makes pursuing other, higher-level political and social values possible. Essentially, like power, it is a relationship between actors, as well as actors and structures (Williams 2008, 6).

In practical terms, security can be given such characteristics as physical security from harm, security of one’s property, ability to minimise unwelcomed interactions and to move freely. In information security context these have been translated into, for example, physical security of one’s device; confidentiality, integrity and availability of information and its exchange; functioning of both hardware and software as expected; and minimisation of unnecessary use of resources and/or time (e.g. Workman et al. 2013, 4; 7-10). Prevention, detection, responding to or recovering from an attack has been the goal of information security. Cyber security complicates the setting for it also deals with security outside one’s own systems and networks, emphasises the interface of physical and digital, and includes the human
element (users of information). In addition to being a problem for individuals, companies and other organisations, it has been lifted high on the political agenda and defined as a question of national security. Difficulty in cyber security is to accommodate both societal and informational frameworks of security and make them talk to one another in an understandable manner. Regardless of the same terms, these frameworks may have significantly varying meanings for them.

What about the mutual relationship of trust and security? First of all, it is multidimensional. As noted earlier, trust is not an issue in certainty which, again, is often associated with security. When ‘things happen’ in an expected way in expected circumstances the question of trust does not need to be invoked. Certainty replaces it and people usually are secure and feel secure in such setting. Certainty tints both continuing and particular encounters, yet, like trust, it develops through experience and over time. Nevertheless, when something unexpected takes place and certainty shatters the question of trust emerges. In such situation security means that the end results or consequences of the event are not devastating; that they remain the same regardless of the event; that they remain within an acceptable range of variation; or that there will be a quick fix to problems. It is hence essentially a question of resilience. Security may also entail an expectation of a compensation which the one suffering from the unexpected event perceives sufficient. Even non-absolute security thus reinforces trust, yet this cannot be taken for granted. People interpret events differently for which reason even minor security doubts may undermine trust. If people are prone to lose their trust easily or trust was not strong in the first place – as it is with regard to cyberspace – they tend to interpret the event in highly negative terms, feel insecure and revert from interaction.

On the other hand, trust is an important ingredient of security. Doubting everything does not induce security but insecurity, whereas being able to trust creates an environment of security. Security is thus a combination of certainty and trust. With regard to the latter, some kind of calculation of probability takes place when estimations about whether or not to trust and to what extent are being made. This calculation is likely different from the risk calculation (e.g. Limnéll et al. 2014, 108-110) or the calculation of credibility (Press 2005, 8-29), but somewhat close to them and also affects security estimations. It is influenced, for instance, by familiarity with the object of trusting, knowledge about associated threats and risks, expectations and beliefs about what is true and what is not, rumours and previous experiences. Coming to the conclusion that there is little or no room for trust in a situation induces insecurity and turns one towards additional security measures — security through something.

In cyberspace, additional security measures usually mean seeking technological clues about or certificates of security. Gaps in technology are to be fixed with additional technology. The problem is that majority of people are not ‘tech-savvy’ enough so that they would be aware or even interested in familiarising themselves with measures planned to strengthen security in an online environment. Cyberspace is an integral part of our everyday and the technology should just function the way it is expected to regardless of our own online actions. Additional security measures also mean regulation (standards, laws, treaties, good practices and so forth) that try to create rules of the game for cyberspace. These are developed, for instance, by states, international organisations, (international) non-governmental organisations, industry associations, court rulings and technology vendors. People’s
unawareness, conflicting interests and dragging behind technology development are main challenges for enhancing security — and trust — through regulation.

Unawareness about cyberspace and different personal attitudes towards technology seem to have created a somewhat twisted online culture. On the one hand, some people see cyberspace as the biggest curse in contemporary societies and vow to stay as far away from it as possible. However, the Western societies are turning towards more and more technology and, for example, the state presents itself increasingly in the form of varied online services. These services are thus deprived from people who are unable or unwilling to operate in cyberspace. This highly affects their social security. On the other hand, some people adopt online technologies quickly and with little concern about security. They get frustrated if the latest application cannot provide what they want and do not believe that sharing even very personal information online is a security question. If trusting backfires both their online and physical identities may become spoofed or stolen. Of course, these are the two behavioural extremes and most people reside somewhere in between them on the continuum.

In sum, security and trust reinforce one another, but it is impossible to say which one comes first. An important part of being secure is that one can trust what he or she depends on. Nonetheless, it is difficult for trust to evolve in an insecure environment. The importance of addressing the link between trust and security in cyberspace lies in its omnipresence. Cyberspace has become the digital backbone of Western societies which has made its protection crucial — yet simultaneously created a situation in which the security of societies, including national security, depends on functioning cyberspace. The protection of the means on which the society is dependent is dependent on the very same means.

State as a node in the global network society

The evolution of the state after the Second World War allocated many new tasks to it, primarily those related to the provision of welfare services. It thus became more than just a security provider. However, the state transformation has continued ever since. The state has been shrinking and currently, the entire concept is sometimes claimed to be eroding. People’s needs and wants — including those related to security — are claimed to differ so much from one another that a single provider cannot respond to all of them. The private sector has come to substitute the public state in many services, including the production of security. This has been evident in the field of cyber security which has been a playfield for commercial security providers for a long period of time.

According to Castells (2009, 16) the ways the state represents itself and its capacity to act depend on the social structure in which it operates. Thus, the state is a labile construct which both modifies and is modified by its environment. Its transformation and freedom of action are restricted, for instance, by its geographical location, history and culture shared by people living within its borders. In other words, all states do not act or change similarly. Currently, globalisation and gradual emergence of the global network society “both relying on communication networks that process knowledge and thoughts to make and unmake trust (ibid.)” are the most fundamental processes modifying states.
The quick diffusion of cyberspace has, to an extent, detached societies from the state laid framework. For this reason, society needs to be set on the focus of analysis and redefined. According to Castells (2009, 18) this can be done by perceiving state as a reformed network state and society as an intersection of multiple socio-spatial networks (technological, military, economic, political, cultural and so forth) that is constantly in flux. Networks are open-ended and expand or contract on the basis of “compatibility or competition between the interests and values programmed in each network” and into those they come in contact with (Castells 2009, 19). Similarly, each network contains and is structured around a particular discourse which separates it from other networks by constituting it in relation to other, bordering discourses (Foucault 2009). In this setting, the state is only one node among others and part of multiple overlapping networks; “[n]etwork is the unit, not the node” (Castells 2009, 19-20).

Along similar lines Aaltola et al. argue that the meaning and role of the state is transforming. Even if it remains a provider of security, the main object to be secured is changing from territory to flows of different resources (goods, finance, people, information and so forth) that travel through global networks. All states and societies to a varying extent rely on several global flows. This means that securing access to these flows and being able to control who else has access to and from them becomes a defining point with regard to state power. Global flows often originate and end up to state territory. Security and stability of global flows hence relies on states, yet the task of safeguarding them is so vast that they are increasingly accompanied by private, non-state actors. (Aaltola et al. 2014, 11; 17; 27-28; 59-60; also Lewis 2006, 2.) Where Castells emphasises the importance of networks as objects of security, Aaltola et al. highlight the meaning of flows travelling through these networks. These points of views are not contradictory but mutually reinforcing, and both of them exist in contemporary critical information protection discourse.

The network state transforms itself to fit this emerging global framework so that it can still assert sovereignty, define citizenship and govern over foreign nationals in its territory to some extent. This is done primarily through three mechanisms: establishment of networks of states like the European Union or NATO, building of international organisations or institutions to deal with global issues such as the United Nations or the World Bank, and allocation of power to regional or local administrations in order to “come closer to the people”. The actual decision-making takes place in the crossing points of manifold governing networks. Sovereignty and responsibility are shared, governing processes more flexible, and the relationship between the state and its citizens varies which all constitute contradictions and friction to the governing process, yet keep it going. (Castells 2009, 39-40.) In the process, the state needs to give up some of its power. This power does not become relocated, but fuses away in the process (Naim 2013, 1-2; 4-8).

However, the state’s adaption to network environment can also be seen in a different light. Schmidt, for example, tends to perceive the state as an immutable hierarchical entity whose principal adaptation strategy is to attempt imposing hierarchical order on networks, including the Internet. By joining networks the state obtains an ability to influence them and modify them to its advantage. It attempts either to improve its position in a network and potentially gain a hegemonic status or to decrease the importance of the entire network. The main driver to such action is the state’s concern about its potential loss of power in network environment. (Schmidt 2014.) The state hence tries to turn networks
into something it knows how to control. Even if this may be the main adaptation strategy of the state, it needs to be kept in mind that the state changes in the process too.

In a network society, the social structure is made around networks based on utilisation of digitally processed information and communication technologies (Castells 2009, 24) — and reasoned by supporting discourses. Therefore, critical infrastructures (CIs), including critical information infrastructure (CII), which constitute the backbone of contemporary societies and are controlled through cyberspace, have been nationally defined as the most important objects of protection (for example, National Research Council 1999; Lewis 2006). In addition to being controlled and directed through cyberspace, many CIs run on it. Unsurprisingly, the significance of cyber threats has in the past few years become highlighted. This is testified, for example, by the fact that many states have recently put together plans and published strategies addressing cyber security and preparation for cyber-attacks. (For example, the United States 2011, the United Kingdom 2011, Finland 2013; and similarly the European Union 2013.)

The European Commission defines CI as “an asset or system which is essential for the maintenance of vital societal functions”. Damage to it, its destruction or disruption “may have a significant negative impact for the security of the [European Union] and the well-being of its citizens”.7 The definition bases on society, not on the state, which is an important shift in security thinking in international affairs.

Similarly, the United States Department of Homeland Security specifies CI as “the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof”.8 Thus, the conventional differentiation in security thinking between inside and outside becomes blurred in strategy statements also.

CII, again, is information and communication “systems [and networks, services and infrastructures] that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)” (COM[2005] 576 final, Annex 1). They “form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures”. “Their disruption or destruction would have a serious impact on vital societal functions”. (COM[2009] 149 final, 2.) According to Lewis, in the United States there are overall eleven sectors and five key assets defined as critical infrastructures. These include agriculture and food, water, public health, emergency services, defence industrial base, telecommunications, energy, transportation, baking and finance, chemicals and hazardous materials, postal and shipping, as well as national monuments and icons, nuclear power plants, dams, government facilities and commercial key assets. (Lewis 2006, 3.) With little imagination it is easy to see the criticality of functioning CII to all of them.

Through doctrinal work cyber security and CI protection have become constituted as questions of national security. Hence the conceptualisation of national security has been modified from a question of

state to state war towards more holistic question of CI protection. By doing this, the state tries to resort to its traditional source of authority and establish itself as an important, coordinating node in the global network society. Through strategizing cyberspace it gradually moves cyberspace from the primarily commercial sphere it has belonged to since the 1990s (e.g. Greenstein 2001) to security sphere or tries to build a parallel network for governing it. Private companies which have traditionally prevailed in cyberspace need to find ways to accommodate or reject these governmental desires. What the gradually emerging security structure looks like and how it functions will be the always transforming “end-result” of these power struggles. On the other hand, the very same development increases the importance and role of companies and other organisations in national security production.

Regardless of the claims that without governmental regulation cyberspace is the new Wild West, there already exists governance in it. This is primarily executed by loose network structures that worry more about the technical aspects of cyberspace than its national security aspects, like the Internet Engineering Task Force (IETF) or the Internet Corporation for Assigned Names and Numbers (ICANN). By strategizing cyberspace the state tries to bring it under conventional (national and international) governance structures that grant more power to it — reduce the technological in the discourse and material practices constituting cyberspace and increase the political and the military. In this article, it is not stated whether this is a good or a bad thing. While pursuing more power, the state in the eyes of its citizens also accepts a bigger role the provision of trust in cyberspace. If CI and its protection become seen more and more as questions of national security, the state is also presumed to make a bigger effort in enforcing online trust. It becomes its task, for instance, to legislate over the digital world, enforce standards and punish those behaving malevolently online. Thus far this has mainly led to attempts to apply rules and procedures developed for the physical world to the digital world.

Lack of trust in cyberspace and its enhancement through improving cybersecurity

Societies are characterised by particular time-space formations. According to Castells, in the network society those are the space of flows and timeless time. The former refers to “the technological and organizational possibility of practicing simultaneity without contiguity” and to “the possibility of asynchronous interaction in a chosen time, at a distance”. It is made of places connected by communication networks through which information flows and with which it interacts. (Castells 2009, 34.) The latter, again, refers to the network society’s tendency to use information and communication technologies in an attempt to annihilate time by negating sequencing — by compressing time and by blurring the sequence of social practices. Both of them are contradictory to the space of places which is based on local experience and only local sharing. (Castells 2009, 35.)

In more practical terms, there are five defining principles that differ between cyberspace and physical space. These, on their part, enable the space of (information) flows. First of them is time, which both subtracts and expands in cyberspace. The second is the partial irrelevance of physical space and distance. Third, the seeming anonymity which prevails in cyberspace; fourth, asymmetry inherent in the space; and finally, efficiency that cyberspace enables. All these are used by both benevolent and
malicious actors operating in the digital world to their advantage. (Limnéll et al. 2014, 63-72.) The emerging security awareness which holds either networks or the flows they enable as its referent object needs to take these principles into consideration. It needs to find ways to accommodate differing security structures and discourses so that an overall “best possible” security can be attained and people are convinced that trusting cyberspace does not backfire. This is a challenge if the state’s main security strategy is to apply existing regulation and governing models to the digital environment and the actors traditionally strong in online environment cannot influence the development. Old ways of interpreting the world are not efficient when new truths prevail, and moreover, are in constant flux.

The unfamiliar form, actors, functions and fundamental principles that characterise cyberspace — and its relation to the physical world — are both reasons for insecurity in and mistrust felt towards it and consequences of lacking security awareness when constructing it. In addition to all positive opportunities residing in cyberspace, there is also a large malevolent potential. Contemporary discourses and practices used for organising and re-organising complex cyberspace highlight this malevolent potential – threats, risks and vulnerabilities – thus granting more room of manoeuvre for actors traditionally perceived strong in security. Global flows are not only positive things, but also include those of cybercrime, recruitment for terrorism, illegal arms trade and so forth. The interpretation is full of fear; not one likely to induce trust and secure feeling. It also highlights the constant presence of threat. In that sense, the potential option to use emergency means when perceived necessary is not as decisive power resource in cyberspace as it is in the physical world. It is more important to indicate that the threat has been recognised, become accustomed to it and learn to live with it. This may not be the preferred state of affairs, but it is an important part of resilience. The situation may also have a negative impact on national security. If, for example, surveillance – done in the name of national security – is perceived too intrusive by the wider population, it starts to undermine trust felt towards the security actor. This, again, can have a negative impact on national security.

Societies, as traditionally defined, become fragmented by the logic of inclusion/exclusion in global networks and flows (Castells 2009, 25; 34). Some of the state’s power has indeed diffused away. It has become only a node, yet an important one, in networks that enable numerous global flows. The state’s power in a particular question depends on which networks it is perceived to be a node of, how important node it is able to constitute itself as, as well as how the question is framed and articulated. Even with regard to war – the traditional security threat the state faces – the emergence of space of flows makes a difference. “Globalization is about circulation [...] and war is itself a form of interconnection (Barkawi 2006, xii; italics removed)”. Not only is warring dependent on CII, but also represents itself in multiple other global flows. War influences how money circulates, where mass-movements head to, what images are shown on daily news or what people comment on social media. Particularly noticeable this is with regard to what is often called “cyberwar”. Cyberwar – without going into problems related to its definition – crosses many conventional division lines used in security decision-making such as civilian-soldier and peace-war. In addition, it blurs the battlefield by bringing war into societies and close actors namely nothing to with the conflict, that is, into Western homes, work places, utility stores and travel. Way too often it dominates in cyber security discourse turning cyberspace into a space of enmity, suspicion, high risk and anxiety.
Even in the future the state might be the main protector of global flows; yet only one of the protectors and, according to Schmidt, a somewhat restricted security apparatus. It will have, to an extent, lost control over what is happening on its territory, yet trying to control access to the flows. The flows are enabled by C(I)I, majority of which is owned and/or operated by the private sector. The situation requires comprehensive security thinking which tries to incorporate all nodes of global networks – especially the most vital ones; those which stand on the crossover points of several networks and in which decisions influencing all of the networks are being made.

The state will retain a capability to mobilise vast resources and modify the operating environment – but so will other actors too. It will concentrate on organising the protection of CI(s), normalising people’s relationship to cyberspace and educating them to become smart e-citizens, providing welfare services online, legislating over the negative impacts of cyberspace and counteracting multiple threats existing in the digital world – most notably those capable of constructing a threat similar to the physical military threat, cybercrime and terrorism, as we as digital espionage. At its mildest form the threat is a hacktivist, a cracker or a group of hackers. However, the responsibility for overall security production will lie on the shoulders of all actors operating in cyberspace – companies, other organisations and individuals – and whose contribution to re-defined (national) security will be substantial. Majority of cyber security professionals – today and tomorrow – work on the private sector, for which reason cross-sectorial collaboration is a must. These professionals and companies are an important source of innovation, create and protect intellectual property and enable the accumulation of vital know-how.

In order for successful collaboration to take place, the manifold actors need to establish trust towards each other and the technology they operate with. It will be their collective responsibility to reassure each other (and the wider population) about their trustworthiness. This requires varying trust-building measures. Trust in cyberspace is not a monolith. It comprises multiple aspects like trust in e-commerce, trust in actors operating in cyberspace, trust in websites, trust in circulating information, trust that cyber-dependent C(I)I functions well enough in all circumstances and trust in cyberspace per se as a space for free exchange and publishing of opinions. All these need to be addressed adequately. All of them need different approaches in thinking and practices as well as varying combinations of actors building trust. How to safeguard trust in each of its aspects is a part of context-bound decision making that entails both political and financial arm wrestling. The currently prevailing mistrust felt towards the state as well as information and communication technology providers in general needs to be addressed too. Moreover, more equal cooperation and collaboration structures between private and public organisations need to be created because currently there are plenty of complaints about inadequate information exchange between the parties and thus, blocked flows.

Addressing the question of digital trust is a step towards the right direction but not enough. Because we above all trust the human element behind technology and networks, and because trust is basically a relationship between two or more human actors, the humane (moral) question of trust needs to be addressed. We are not yet used to network structures for which reason suspicion towards them prevails. There are calls for and serious attempts to create familiar, hierarchical structures of authority in cyberspace which would make it easier to point out those responsible when something does not go the way expected. However, as cyberspace is not the same thing as physical space and because it is
governed by different kind of defining principles, questions of security and trust need to be addressed through a combination of different means. Technology should not be perceived an obligating, external force over which there is little influence but a time and space specific expression of societal, cultural and political values. It is neither a bugbear to be afraid of nor a value-free solution to problems but an expression of moral and political choices. People will only begin trusting cyberspace if it functions as expected or if they know how it functions and thus are willing to accept more uncertainty with it.

Mistrust in cyberspace does not only hinder collaboration, but also feeds inefficiencies and suspicion, creates problems of management and governing, whereas trust facilitates interaction, reduces risk and increases predictability. All latter are important ingredients of security. Without the necessary level of trust many cross-national problems remain unaddressed; without it the normalisation practices that turn cyberspace into a space that one feels secure to act in are either based on misperception or do not work. Mistrust felt towards the backbone of contemporary Western societies spreads insecurity and uneasiness, yet at the same time serves as a self-protective and self-preserving mechanism. While retaining healthy, critical way of thinking is desirable, it needs to be acknowledged that restoring trust through enhancing security serves the interest of the majority. It increases security of the society in general.

In the global network society security focus needs to be on flows and critical infrastructures, diffusion of different border-lines, resilience, collaboration, and on re-formed, comprehensive awareness. The reformed way of thinking needs to be incorporated in varying managing and governing structures and procedures of which many aim at providing security or reinforcing trust. The state does this by establishing networks of states, building international organisations and institutions, as well as by allocating powers both up- and down-wards. It can also use market mechanisms, for example, purchasing power or creation of incentives for companies, other organisations and individuals to invest in cyber security. (For details, for example, Eronen 2014.)

Companies and organisations can reinforce trust by participating selectively in collaborative structures and information sharing, taking care of their own equipment, networks and procedures as well as influencing those of their partners’, educating and training their personnel and participating in market self-regulation and standardisation. In business terms, by “building trust you will be able to maximise your growth potential and manage the risks in the opportunities available in the digital age. Trust means your customers will buy your products on-line. It means they’re confident you’ll keep their data safe and secure. Trust means your suppliers know your systems won’t fail them. And it means you have the confidence to move your business forward by embracing technology and the opportunities it has to offer”. (PWC 2013, 4.)

When securing critical infrastructures, networks and flows it is important to make it clear which are the referent objects, threats and related means of security production in each particular question, who is to address them and how collaboration is to be structured. Societies through which global flows travel are able to influence these flows but also become transformed by them. Currently, cyberspace is the main space in and through which influencing takes place for which reason security in and trust felt towards it are crucial societal questions. What we do not want to witness in the future is the constant flow of
studies according to which 67 per cent of respondents agree with the statement that technology companies “have violated the trust of users by working with the government to secretly monitor communications of private citizens” (WeLiveSecurity 9.4.2014). 

---

9 The survey was conducted online within the United States by Harris Poll on behalf of ESET from February 4-6, 2014 among 2,034 U.S. adult adults ages 18 and older, among which 1,691 are at least somewhat familiar with the NSA revelations. This online survey is not based on a probability sample and therefore no estimate of theoretical sampling error can be calculated.
Bibliography


