UI Occasional papers
#23
DECEMBER 2013
PUBLISHED BY THE SWEDISH INSTITUTE OF INTERNATIONAL AFFAIRS. WWW.UI.SE

A RESILIENT EUROPE FOR AN OPEN, SAFE AND SECURE CYBERSPACE

egs | TOWARDS A EUROPEAN GLOBAL STRATEGY 2013

REPORT BY
DR. MYRIAM DUNN CAVELTY
Head of Risk & Resilience Research Group Center for Security Studies (CSS), Zurich / Switzerland

TABLE OF CONTENTS

INTRODUCTION

Without a doubt, cyber-security is the policy-issue of the hour. The cyber-attacks on Estonia in 2007; the discovery of Stuxnet, the industry-sabotaging super worm in 2010; numerous instances of cyber-espionage, culminating in the Snowden revelations this year; and the growing sophistication of cyber-criminals as evident by their impressive scams have all combined to give the impression that cyber-attacks are becoming more frequent, more organised, more costly, and altogether more dangerous. In short, cyber-threats and the measures necessary to counter them are considered a top priority in more and more states around the world, including many European countries.[1] As a result of increasing attention particularly on the national security aspect of the topic, the amount of money spent on defence-related aspects of cyber-security is rising worldwide (Brito and Watkins 2011; Boulanin 2013).

Indeed, we are now at a point in world history where any political power with global aspirations needs to partake in the cyber-game. The last few years have made abundantly clear that cyber-issues permeate (almost) everything: information technology is fast becoming the common underlying factor upon which more and more security issues converge. There are enough indications, for those willing to listen, that the risk of a severe cyber-attack is very low (Rid 2013; Sommer and Brown 2011). However, even the lowest of probabilities that strategic cyber-war may ever become reality is sufficient to keep the defensive and offensive cyber-war preparations going. As a result, any Grand Strategy or security strategy needs to consider cyber-issues today. The apt observation that "the European Union may well avoid debating strategy, but as a foreign policy actor it cannot avoid doing strategy in the real world, like it or not" (Biscop 2012: 1) should thus be expanded by adding "… and it cannot avoid doing strategy with regards to the cyber-world".

Such a cyber-strategy needs to have at least two elements: First, any global power needs to be able to "defend" against cyber-threats, or rather, manage them adequately, while striving to be and ultimately become, (cyber-)resilient. Second, a global power needs to wield some sort of cyber-power, but, as will be shown, a very specific "soft" (but of course not inferior) one, if the vision of an open, safe, and secure cyberspace is to be obtained. Both these necessities, internal cyber-resilience and external cyber-power, build on each other: there cannot be any true cyber-power without cyber-resilience – and vice versa. In the context of the European Union, both aspects will have to be influenced by the core values on which the EU itself and all of its domestic policies are based, i.e. be preventive, holistic and multilateral, and it must contribute to the vision that the EU should be "ready to share in the responsibility for global security and in building a better world" (European Security Strategy 2003: 1).

TOWARDS A CYBER-RESILIENT EUROPE

In the contemporary political debate, some objects – commonly called infrastructures – and the functions they perform are regarded as 'critical' by the authorities (in the sense of 'vital', 'crucial', 'essential') because their prolonged unavailability harbours the potential for major crisis, both political and social (Burgess 2007). In the mid-1990s, the issue of cyber-security was persuasively interlinked with this topic of critical infrastructures and their necessary protection (PCCIP 1997). It was established at that time that key sectors of modern society[2], including those vital to national security and to the essential functioning of industrialized economies are vulnerable, because they rely on insecure national and international software-based control systems for their smooth, reliable, and continuous operation.

From a security perspective, the key challenge in this domain arises not only from a "new" type of amorphous threat which is immune to most of the classical security measures, but also from the privatization and deregulation of large parts of the public sector since the 1980s and the globalization processes of the 1990s, which have put many critical infrastructures in the hands of private (transnational) enterprise. A situation arises in which market forces do not provide a sufficient level of security and state and supranational actors are also incapable of providing the level of security they want on their own; they are forced to exert indirect influence by intervening with regulation, offering incentives, or seeking other types of cooperation with infrastructure operators (Dunn Cavelty and Suter 2009). Like so many other political entities, the European Union has been dealing with cyber-related issues for a number of years (Klimburg and Tirmaa-Klaar 2011) – with varying success.

THE EU'S CURRENT APPROACH TO CYBER-IN-SECURITY

Until 2007, the EU's approach to cyber-security was framed mainly as sub-category and side issue of the efforts to stimulate and secure the development of an Information Society in Europe. After the 2007 Estonian attacks[3], the European Commission started to tackle the issue of significant cyber-attacks as a security issue on its own right (European Commission 2009), steadily building up a body of Directives and Regulations with bearing on cyber-issues. Most recently, the European Commission released its own Cybersecurity Strategy, entitled "An Open, Safe and Secure Cyberspace", paired with a somewhat bold Directive ("The NIS Directive") that offers to tackle some of the core problems of cyber-security governance (European Commission 2013a, 2013b).

There are a variety of bodies working in the field of cyber-security, such as the European Network and Information Security Agency (ENISA), the European Public–Private Partnership for Resilience (EP3R), the Computer Emergency Response Team (CERT) for EU institutions, or the EU Cybercrime Centre within Europol. It is, indeed, not easy to understand "who talks to whom and how co-ordination and co-operation is achieved" and how all the different pieces fit together (Robinson et al. 2013: 96). Still, despite a relatively fragmented policy set-up, the EU's strategy for internal cyber-resilience cannot be criticised for its fundamentals. A rather pragmatic, level-headed approach has emerged over the years, in which two principal policy areas can be distinguished.

First, there are measures to ensure 'Network and Information Security' (NIS) to support Critical (Information) Infrastructure Protection (CIP or CIIP). These measures are mainly about standardizing risk management, but there are serious considerations to establish a broad security incident reporting mechanism in the NIS Directive. Second, there are measures intended to combat cyber-attacks of all sorts, including large scale ones, with a main focus on cyber-crime activities. Here, the main thrust in the spirit of the Budapest Convention is the harmonization of cyber-law in Member states, the improvement of operational law enforcement cooperation as well as political cooperation and coordination among Member States, i.e. in the field of information exchange. There is a third potential focus on military aspects of cyber-security, but while

the EU has a nascent cyber-defence concept for 'Common Defence and Security Policy' missions and the European Defence Agency (EDA) is developing cyber-defence capabilities and technologies, cyber-defence at the EU level is not a priority (Simon 2010; Klimburg and Tirmaa-Klaar 2011: 34), even though that aspect has been strengthened in the new Cybersecurity Strategy (European Commission 2013a: 11). The EU is also striving to intensify cooperation with NATO in cyber-security in coming years.

That said, are these approaches sufficient to ensure the necessary level of cyber-resilience in Europe? In theory, yes: The European approach to cyber-security could be considered a best-practise approach, at least on paper. In practice, however, cyber-security or rather, cyber-resilience is very hard to obtain. There are several interrelated reasons for why this policy issue is so hard to tackle, some of which are discussed below.

RISK ASSESSMENT (AND ITS FLAWS)

In the NIS/CIIP field, the key institutional actor in the EU is the European Network and Information Security Agency (ENISA), which is supervised and financed by DG CONNECT. ENISA stands for the propagation of (standard) information assurance practices, geared towards the management of risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes (May et al. 2004). While risk assessment methodologies have a long tradition in cyber-security, they are also fundamentally flawed in the context of complex networks and complex risks, because they build on linear methods, whereby an extrapolation into the future is done on the basis of past experience.

As long as cyber-security issues have been on the political agenda, the debate has been characterized by the struggle of various practitioners and security specialists to determine how big the threat really is (Dunn Cavelty 2008). The main reason for this is that there is an incomplete view of the frequency and gravity of cyber-incidents in individual companies and in government networks, i.e. because these actors do not have sufficient incident detection capabilities or because they are not forthcoming with the information. Therefore, there is even far less knowledge about the exposure in whole business sectors, let alone on an aggregated level of countries, much less on the level of the EU. Attempts to collect and aggregate data beyond individual networks have failed due to insurmountable difficulties in establishing what to measure and how to measure it and what to do about incidents that are discovered very late, or not at all (Sommer and Brown 2011: 12; Suter 2008; Robinson et al. 2013: 58). Reports that try to aggregate on the level of countries, published by IT (security) companies or other specialized consultants, have been called a "sales promotion exercises" (Espiner 2011) and questioned for their methodology (Maass and Rajagopalan 2012; see also Ryan and Jefferson 2003; Anderson et al. 2012; Florencio and Herley 2011). The data problem, which translates into a policy problem because clear prioritization become impossible, is well recognized, which explains the main thrusts of the NIS Directive towards mandatory incident reporting (with unsure benefits).

Given that there is not even agreement on how large the threat is today, it is hardly surprising that experts even more widely disagree on how it will develop in the future. That comes with struggles to identify the most important threat "form" and who should get the resources to counter it. While there is at least proof and experience of cyber-crime, cyber-espionage or other lesser forms of cyber-incidents on a daily basis, cyber-incidents of exceptional impact exist exclusively in the form of stories or narratives. Establishing the likelihood of such an occurrence is impossible. Large-scale or "systemic" cyber-risks are unpredictable and incalculable due to the uncertainty surrounding them. The complexity of the socio-technical environment that they co-create makes traditional linear risk management approaches ineffective. This is also the main reason for the rather rapid spread of another concept in security-politics: resilience.

RESILIENCE: BEYOND THE LIMITS OF RISK ANALYSIS

Resilience is commonly defined as the ability of a system to recover from a shock, either returning back to its original state or to a new adjusted state (Perelman 2007). This concept goes well beyond risk management, as it no longer assumes that all risks can be avoided or at least reduced to an acceptable level if they are properly managed. Infrastructure resilience reduces the magnitude, impact or duration of a disruption. Instead of calculating the likelihood

and potential impact of risks, a resilience approach focuses on the analysis of the system itself and tries to design protection measures that are independent from the type and extent of risk. This also shifts the focus of attention away from the preventative towards the response and recovery phase of disaster management (Duit et al. 2010).

If resilience is a core concept, security does not refer to the absence of danger but rather the ability of a system quickly and efficiently to reorganise to rebound from a potentially catastrophic event. Adaptability and flexibility are common characteristics found within a high-resilient system. Furthermore, such systems are robust (they have the capacity to withstand stress); there is redundancy (alternative options are available to a distressed system); and they are resourceful (the system has the capacity to mobilize and respond to an emergency). This also means that resilience approaches privilege self-organized governance from within the system rather than by hierarchically superior actors outside the system. Through this lens governance is conceptualized as a shared process, ultimately creating greater complexity in the administration of public goods (Boin and McConnell 2007).

ENISA, the key player in cyber-security, also calls for "sound and implementable preparedness, response and recovery strategies" in connection with resilience, and there are initiatives like the European Public Private Partnership for Resilience (EP3R) that have a particular focus on this concept. The new Cybersecurity Strategy is all framed in the language of resilience, too (European Commission 2013a: 5ff).

However, while resilience is recognized as a crucial element of cyber-security, there also are relatively little specific efforts to operationalize and implement it. The EU is not alone in this: it is one of the bigger issues related to resilience-approaches world-wide. If resilience is to be applied in a targeted and gainful manner, four issues must be dealt with in practical terms: Political actors need clarity about the nature of the desired resilience; the goals of resilience policy; the concrete instruments to be used in fostering resilience; and the question of how to measure current and future resilience levels (for more details on these points see Dunn Cavelty and Prior 2013). If Europe wants to be or rather become cyber-resilient, it must look at these questions sooner rather than later and in much more detail.[4]

In the context of global power politics, there is an additional function of resilience: resilience is seen by many as the key for cyber-deterrence (Gearson 2012; Libicki 2012; Demchak 2011). Clearly, a political entity that can show that its people are sufficiently agile and its capabilities sufficiently robust against all manner of disasters also demonstrates similar immunities to disasters from cyberspace. While it will be impossible for this political entity to ever demonstrate an ability to block and/or neutralize cyber-attacks, it may be able to prove that its missions can succeed even though the attack worked. In the nascent cyber-deterrence literature, the best dissuasion against a potential cyber-war in the future is deterrence by denial: by demonstrating that a major cyber-attack is ultimately of little consequence. This, in turn, makes (internal) resilience an element of power – the focus of the next chapter.

THE EU AS CIVILIAN CYBERPOWER

Today, a global power needs the ability to be cyber-resilient against cyber-incidents but it also needs the ability to project power in cyberspace and to shape the global cyber-security landscape. In its new Cybersecurity Strategy, the European Commission brings under one framework internal market, justice and home affairs and foreign policy angles of cyberspace issues, thereby attempting to co-ordinate policy across three areas whose competences and mandates were formerly very separate: law enforcement, the 'Digital Agenda', and defense, security, and foreign policy (Robinson 2013). It takes a clear stance with regards to the external dimension, which is in line with the EU's overall values. The message in the Strategy is that the EU wants to promote cyberspace as an area of freedom and fundamental rights. This includes expanding access to the Internet as a tool to advance democratic reform worldwide – but without an increase of censorship or mass surveillance. The EU states that an important pre-condition for free and open Internet that brings political and economic benefits to societies, is to maintain a multi-stakeholder governance model of the Internet. It sees the "preservation" of an open, free and secure cyberspace as a global challenge, which the EU wants to address together with the relevant international partners and organisations, the private sector and civil society (European Commission 2013a).

As timely and welcome as the EU's Cybersecurity Strategy is, it also is a product of the pre-Snowden cyber-era. While nothing it contains is in any way discredited by the NSA revelations this year, they have nonetheless led to a substantial correction of many aspects of the cyber-security discourse and the way cyber-threats are perceived. In general, the pre-Snowden era was strongly influenced by a belief in the positive transformative powers of the Internet. There was a lot of hope that digital tools would diffuse power down to the traditionally weak, by giving them a place to coordinate and communicate efficiently and anonymously, which would also have a democratising effect. What has become clear, however, is that cyberspace is the site of an "epic" power struggle in which democracy, freedom and fundamental rights play little to no role – with potentially detrimental effects on cyberspace as we know it. This, in turn, is putting very specific constraints on the EU's ability and necessity to project power in cyberspace; but also opens up new opportunities for a very specific role.

THE OPEN, SAFE, AND SECURE CYBERSPACE IS UNDER ATTACK

While the possibilities of instant, distributed communication has definitely changed many aspects of our lives substantially and has had an effect on how we conceptualise power today, traditional "state" power is back with a vengeance (if it was ever gone) (Schneier 2013). A type of "feudal security" consolidates power in the hands of the few: IT companies, most of them American, can act almost exclusively in their own self-interest, changing social norms by accident or deliberately, at all times using "the users" to increase their profits (Schneier 2012). Also, an increasing number of governments are controlling what their citizens can and cannot do on the Internet. Totalitarian governments are embracing a growing "cyber-sovereignty" movement to further consolidate their power. But democratic states are doing very similar things: There is more government surveillance, more government censorship, and more government propaganda than ever before (Deibert 2013).

As a consequence, the vision of an open, safe, and secure internet is under attack from all sides. Many nations are increasingly zooming in on the strategic-military aspects of cyber-security. This means to subject the issue to the rules of an antagonistic zero-sum game, in which one party's gain is another party's loss. It invokes images of adversaries, is focused on national security measures instead of economic and business solutions, and suggests that states can (and must) establish control over cyberspace. Contrary to the beliefs of cyber-utopians, such control is possible, at least in part: Cyberspace, unlike the air, space, or the sea, is an entirely man-made realm, at all times shaped by economic and political forces (Deibert

et al. 2008). If cyberspace is conceptualized as an unruly place that needs to be tamed at all costs, then this inevitably leads to strong(er) interference of states into the global cyber-system, including the topology of the Internet (Mueller et al. 2013).

Inevitably, such assertion of state power links the discussion of security in cyberspace to the possibility (and desirability) to create borders in cyberspace. Concepts such as Cyber-Westphalia tap into the founding myths of a stable political world order and invoke the closured, safe cocoon of a delimited and thus defendable and securable place, newly reordered by the state as the sole real guarantor of security, whereby 'the topology of the Internet, like the prairie of the 1800s' American Midwest is about to be changed forever—rationally, conflictually, or collaterally—by the decisions of states' (Demchak and Dombrowski 2011: 32). In this view, the process of re-establishing control in cyberspace is seen as inevitable, because security is the most basic need of human beings and seeking security will triumph over other, lesser, inferior needs (such as privacy). Furthermore, the more the issue is presented like a traditional national security issue, the more natural it seems that the keeper of the peace in cyberspace should be the military. The more the issue is based on (traditional, co-ercive) state-power, the more easily it can be governed by traditional (and fairly well-proven) instruments of security, including international laws, norms, or the logic of deterrence.

There is a certain appeal to this image, where the unruly and dangerous "dark" side of cyberspace is kept "outside", and relative security, and with it, prosperity, can be established among states globally. However, another likely possibility is that such a process would result in the further and sustained 'Balkanization' of the Internet (Frieden 1998). This process has so far been tied to totalitarian regimes like China and its "Great Firewall" or more recently, to Iran, which blocks most social media sites and is currently developing its own "Internet". However, the practices of US intelligence services have given similar ideas credence in democratic states like Brazil or Germany, which are all discussing "national" solutions in order to make their communication systems impossible to tap into from the outside (Brown 2013). From the perspective of individuals without much technological prowess, the cyberspace that is likely to emerge from this process will be a place in which netizens will fall "under a complex array of different jurisdictions imposing conflicting mandates and conferring conflicting rights" (Meinrath 2013). In other words, cyberspace will no longer be "one" space, but there will be different "nets", each with their own standards, controlled directly or indirectly by state actors. It is very likely that such a development will come with considerable challenge to anonymity in cyberspace – and will definitely be the opposite of an "open" cyberspace (though it may be more secure for some).

SECURITIZATION / MILITARIZATION OF CYBERSPACE

There is another trend that is directly challenging the EU's vision of an open, safe, and secure cyberspace. The sustained, even increased focus on national security aspects of the topic has led – partially at least – to what security scholars call "securitization": a political process in which political issues are turned into security issues (Buzan et al. 1998). The often-undesirable aspect about such a process from an ethical and societal perspective is that a successful securitization legitimizes exceptional measures beyond the "normal bounds of political procedure" (Buzan et al. 1998: 24). This could include declaring a state of emergency, attacking another country, but also subjecting the issue to the realm of secrecy. In short, it is about breaking otherwise binding rules or governing by decrees rather than by democratic decisions. This, in turn, opens the door for power abuse, disregard for civil liberties, and therefore, ultimately, negative implications for the security of citizens.

An additional dimension with implications for the security of citizens arises from state practices that use cyberspace for mass surveillance, which is helped by the aforementioned trend. In this day and age, more and more user or system specific data is up for grabs – for anybody who is interested in it, ranging from business, to criminals, and the intelligence services. While just the extensive data collection by companies and intelligence agencies (for differing reasons) is already a cause for concern, the consequences of this for the security of citizens becomes fully apparent when the possibilities of its analysis are taken into account. With a relatively simple network analysis, detailed insight into the private lives and relationships of each individual can be gained. More sophisticated methods of

calculation are less interested in the present but are geared towards the prediction of future behaviour (and motivations) of people, using the masses of data available. Such techniques are already used for targeted advertising, whereby an algorithm defines that if Person X buys this or that product, it is very likely that X is also interested in this or that product. In predictive policing, similar techniques are used to calculate crime hot spots. A goal of intelligence services is to be able to have advance warning of i.e. radicalization or terrorist behaviour, based on data combination that could look like this: If Person X visit this website and that website, is in contact with this and that person and has this specific motion profile, then it is likely that Person X will commit a terrorist attack in the next 2 years.

From a data protection perspective, these developments are daunting, particularly because the so-called commercialization of data is not done against the wishes of the user, but rather because it seems to make our lives so much more efficient and convenient. Sure, targeted advertising is at best intrusive and is far from constituting a direct threat to citizens. However, much more unpleasant implications of individual risk profiles are already apparent today, with people being excluded from certain services, because aspects of their (private) life does not meet the requirements of a company. In the future, it is not unlikely that even more unpleasant and more directly political relevant implications arise when democratic rights, such as political dissidence, are seen as an opportunity for government intervention in the sense of "proactive security" (i.e. at airports).

That said, the security-implications go much further. It has been suspected for a while and is now confirmed that the intelligence services of this world are making cyberspace more insecure directly; in order to be able to have more access to data, and in order to prepare for future conflict. It has been revealed that the NSA has bought and exploited so-called zero-day vulnerabilities in current operating systems and hardware to inject malware into numerous strategically opportune points of the Internet infrastructure (Greenwald and MacAskill 2013). It is unknown, which computer systems have been compromised – but it is know that these backdoors or sleeper programs can be used for different purposes (surveillance, espionage, disruption, etc.) and activated at any time. In addition, it has been revealed that the US government spends large sums of money to crack existing encryption standards - and apparently has also actively exploited and contributed to vulnerabilities in widespread encryption systems (Simonite 2013).

The crux of the matter is that intelligence backdoors reduce the security and resilience of the entire system – for everyone. The exploitation of vulnerabilities in computer systems and the weakening of encryption standards have the potential to destroy trust and confidence in cyberspace overall. Furthermore, there is no guarantee that whoever inserts the backdoors has full control over them and/or can keep them secret – in other words, they could be identified and exploited by criminal hackers or even "terrorists". Here, state practices not only become a threat for the security of citizens: paradoxically, they also become a threat for themselves.

NEEDED: A DIFFERENT VISION OF CYBER-POWER

This new twist in the cyber-security debate has rather substantial implications for a cyberspace that is envisaged as an area of freedom and fundamental rights. If the European Union wants to project power in cyberspace without becoming untrue to its values, goals, and core principles, it must necessarily stand for a type of cyber-power that does not fall into the trap outlined above: the trap that the quest for more security in and through cyberspace based on traditional modes of national security thinking and power projection leads to less security, less openness, and less safety for everyone.

Overall, cyber-power is an elusive concept. By US scholars, it has mainly been defined as an addition to the already existing hard (and soft) power toolset (Nye 2010), for example as an ability to use cyberspace to create specific political advantages, mainly by influencing events in all the other operational environments and across all the other elements of power (Kuehl 2009). While such a definition is certainly useful in the context of a traditional understanding of (military) power, it also particularly focuses our attention on aspects of power that are (more or less) coercive. This type of power is often conceptualized as a win-lose kind of relationship. Having that power means taking it from someone else, and then, using it to dominate

and prevent others from gaining it (VeneKlasen and Miller 2002: 39). Clearly, this kind of power is not to the benefit of everyone, but only to the power-wielder. In the cyber-security debate, coercive power is tied to offensive cyber-tools (or 'cyber-weapons') and cyber-attacks – and we are back to the security-trap outlined above. Any potential strategic benefits notwithstanding, the use of offensive cyber-weapons – outside of a few very clearly defined defensive situations – is morally, ethically, and legally questionable in many cases and has a potentially negative impact on the security of citizens worldwide. Therefore, such a cyber-power is in direct opposition to an open, safe, and secure cyberspace and is not a domain the EU should venture into.

However, power cannot just be expressed in coercive ways, but is much more multi-faceted. Ever since Joseph Nye coined the term "soft power", the more cooptive or convictive use of power has become an important element of modern politics. In other words, we are talking about a distributed power built on the strength of various human (and organizational) elements existing with relation to cyberspace. First of all, such a cyber-power builds on "the coordination of operational and policy aspects across governmental structures [and] coherency of policy through international alliances and legal framework" (Klimburg 2011b: 43). More importantly still, it is a type of power that is based on mutual support, solidarity and collaboration, draws on the strength of the private sector and civil society and is directly related to the "ability of a government apparatus to work together with non-state actors" such as infrastructure operators, programmers, researchers, hackers, etc. (Klimburg 2011a: 175). Thus, the type of cyber-power that the European Union needs is expressed through finding common ground between the different stakeholders involved and by building collective strength with and among these stakeholders. And here, we come full circle: this type of power is directly linked to the concept of resilience, and through the concept of resilience, to more security.

CONCLUSION – THE WAY FORWARD

As Bruce Schneier has so aptly observed, we are now only at the very beginning of some critical debates about the future of the Internet. In particular, the year 2013 saw considerable change in threat perceptions, when cyber-attacks suddenly took a backseat, and issues of cyber-exploitation by states came to the foreground. The issues on the table are "the proper role of law enforcement, the character of ubiquitous surveillance, the collection and retention of our entire life's history, how automatic algorithms should judge us, government control over the Internet, cyberwar rules of engagement, national sovereignty on the Internet, limitations on the power of corporations over our data, the ramifications of information consumerism" etc. (Schneier 2013).

Without a doubt, we are at a critical junction in cyber-security policy making. In other words, a set of state practices, ranging from mass surveillance to nationalization of cyberspace, coupled with the interests of private companies, are making the virtual world overall less and not more secure for their citizens. This is a paradox and a dilemma, when considering that the overall aim of cyber-security policies worldwide is to reduce the risks in and through cyberspace. In particular, what becomes exceedingly clear from the developments and lessons of the last few decades is that a strategically exploitable cyberspace is quite the opposite from a secure and resilient cyberspace. Everything currently points to the need to make a choice for either the one, or the other – it does not seem that there is a solution that aligns both interests.

The European Union has already made a choice for an open, safe and secure cyberspace. As a global power, the European Union needs to stand for this vision – and actively counter other tendencies that have become apparent. To be the herald for an open, safe and secure cyberspace, the European Union needs cyber-resilience to withstand cyber-risks of all sorts. This goal is hard to reach, but the existing problems are known and the many of the solutions are identified. Furthermore, the European Union needs to become the wielder of a type of cyber-power that is based on the same bottom-up, distributed forces that resilience builds on. This way, Europe can be a powerful actor in the cyber-realm and can set a benchmark on cyber-security for the rest of the world to follow.

BIBLIOGRAPHY

Anderson, Ross et al. (2012) 'Measuring the Cost of Cybercrime', Research Paper, available at http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf (accessed on 29 November 2013).

Biscop, Sven (2012) 'Raiders of the Lost Art: Strategy-Making in Europe', *Egmont Security Policy Brief*, No. 40, November, available at http://www.europeanglobalstrategy.eu/upl/files/79183.pdf (accessed on 29 November 2013).

Boin, Arjen and Allan McConnell (2007) 'Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience *Journal of Contingencies and Crisis Management* 15 (1): pp. 50 – 59.

Boulanin, Vincent (2013) 'Cybersecurity and the arms industry'. In: SIPRI Yearbook 2013: Armaments, Disarmament and International Security. Oxford: Oxford University Press

Brito, Jerry & Tate Watkins (2011) 'Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity', Policy Mercatus Center George Mason University, Working Paper No. 11-24, April 2011.

Brown, Hayes (2013) 'How The NSA Leaks Could End The Internet As We Know It', Think Progress, 25 October. Available at: http://thinkprogress.org/security/2013/10/25/2836421/nsa-leaks-end-internet-know/ (accessed on 29 November 2013).

Burgess, Peter (2007) ,Social values and material threat: the European Programme for Critical Infrastructure Protection' *International Journal of Critical Infrastructures* 3(3-4): pp. 471–487.

Buzan, Barry, Ole Wæver, O. & Jaap de Wilde (1998) *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.

Deibert, R.J., Palfrey, J.G., Rohozinski, R. & Zittrain, J. (2008). *The Practice and Policy of Global Internet Filtering*. Cambridge: MIT Press.

Deibert, Ronald (2013) *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart.

Demchack, Chris (2011) *Wars of Disruption and Resilience: Cybered Conflict*, Power, and National Security Conflicts, Athens: University of Georgia Press

Demchak, Chris & Peter Dombrowski (2011) 'Rise of a Cybered Westphalian Age' *Strategic Studies Quarterly*, Spring, 32-61.

Duit, Andreas, Victor Galaz, Katarina Eckerberg and Jonas Ebbesson (2010) 'Governance, Complexity, and Resilience' *Global Environmental Change* 20(3): pp. 363 – 368.

Dunn Cavelty, Myriam & Manuel Suter (2009) 'Public-Private Partnerships are no Silver Bulled: An Expanded Governance Model For Critical Infrastructure Protection' *International Journal of Critical Infrastructure Protection* 2(4): pp. 179–87.

Dunn Cavelty, Myriam (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge.

Dunn Cavelty, Myriam and Tim Prior (2013) 'Resilience in Security Policy: Present and Future' *CSS Analysis in Security Studies*, No. 142. Available at http://www.css.ethz.ch/publications/pdfs/CSS-Analysis-142-EN.pdf (accessed on 29 November 2013).

Espiner, Tom (2011) 'Cybercrime cost estimate is 'sales exercise', say experts', ZDNet, February 18, 2011. Available at: http://www.zdnet.com/cybercrime-cost-estimate-is-sales-exercise-say-experts-3040091866/ (accessed on 29 November 2013).

European Commission (2009) Communication 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM (2009)149.

European Commission (2013a) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013)1final.

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, 2013/0027(COD).

European Security Strategy (2003) A Secure Europe in a Better World. Brussels.

Florencio, Dinei and Cormac Herley (2011) 'Sex, Lies and Cybercrime Surveys', Microsoft TechReport, available at http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf (accessed on 29 November 2013).

Frieden, Rob (1998) 'Without Public Peer: The Potential Regulatory and Universal Service Consequences of Internet Balkanization' *Virginia Journal of Law and Technology*, 3(8) Available at www.vjolt.net/vol3/issue/vol3_art8.pdf (accessed on 29 November 2013).

Gearson, John (2012) 'Deterring Conventional Terrorism: From Punishment to Denial and Resilience' *Contemporary Security Policy* 43(1): pp. 171-198.

Greenwald, Glen & Ewen MacAskill (2013) 'Obama orders US to draw up overseas target list for cyber-attacks', The Guardian, 7 June 2013. Available at http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas (accessed on 29 November 2013).

Klimburg, Alexander (2011a) 'The Whole of Nation in Cyberpower', *Georgetown Journal of International Affairs*, Special issue: International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity, 171-179.

Klimburg, Alexander (2011b) 'Mobilising Cyber Power' *Survival* 53(1): pp. 41-60.

Klimburg, Alexander and Heli Tirmaa-Klaar (2011) Cybersecurity and Cyberpower : Concepts, Conditions and Capabilities for Cooperation for Action within the EU, Study for the Directorate-General for External Policies of the Union, EXPO/B/SEDE/FWC/2009-01/LOT6/09.

Kuehl, Dan (2009) 'From Cyberspace to Cyberpower: Defining the Problem', in: Franklin D. Kramer/Stuart H Starr/Larry K Wentz (eds.): Cyberpower and National Security.

Libicki, Martin (2012) *Cyberdeterrence and Cyberwar*, Santa Monica: RAND.

Maass, Peter and Megha Rajagopalan (2012) 'Does Cybercrime Really Cost $1 Trillion?', ProPublica, 1 August 2012. Available at: http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion (accessed on 29 November 2013).

May, Chris et al. (2004) 'Advanced Information Assurance Handbook', CERT®/CC Training and Education Center, CMU/SEI-2004-HB-001. Pittsburgh: Carnegie Mellon University.

Meinrath, Sascha (2013) 'We Can't Let the Internet Become Balkanized: The backlash to U.S. surveillance threatens the foundation of a free and open Web', Slate, 14 October 2013, available at: http://www.slate.com/articles/technology/future_tense/2013/10/internet_balkanization_may_be_a_side_effect_of_the_snowden_surveillance.html (accessed on 29 November 2013).

Nye, Joseph (2010) *Cyber Power*, Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School. Available at http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (accessed on 29 November 2013).

PCCIP President's Commission on Critical Infrastructure Protection (1997) *Critical Foundations: Protecting America's Infrastructures*. Washington: US Government Printing Office.

Perelman, Lewis J (2007) 'Shifting Security Paradigms: Toward Resilience', in J.A. McCarthy (ed.) *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*. Washington: George Mason University.

Rid, Thomas (2013) *Cyberwar will not take place*. Oxford: Oxford University Press.

Robinson, N., Horvath, V., Cave, J. Roosendaal, A. (2013) Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts, Committee on Industry, Research, and Energy.

Robinson, Neil (2013) 'The European Cyber Security Strategy: Too Big to Fail?', Available at: http://www.rand.org/blog/2013/02/the-european-cyber-security-strategy-too-big-to-fail.html (accessed on 29 November 2013).

Ryan, Julie and Theresa Jefferson (2003) 'The Use, Misuse, and Abuse of Statistics in Information Security Research', Research Paper. Available at: http://attrition.org/archive/misc/use_misuse_abuse_stats_infosec_research.doc (accessed on 29 November 2013).

Schneier, Bruce (2012) 'When It Comes to Security, We're Back to Feudalism' Wired, Available at: http://www.wired.com/opinion/2012/11/feudal-security/ (accessed on 29 November 2013).

Schneier, Bruce (2013) 'The Battle for Power on the Internet', The Atlantic. Available at: http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824 (accessed on 29 November 2013).

Simonite, Tom (2013) 'NSA's Own Hardware Backdoors May Still Be a "Problem from Hell"', MIT Technology Review. Available at: http://www.technologyreview.com/news/519661/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/ (accessed on 29 November 2013).

Sommer, Peter & Ian Brown (2011) Reducing Systemic Cyber Security Risk, Report of the International Futures Project, IFP/WKP/FGS(2011)3. Paris: OECD.

Suter, Manuel (2008) 'Improving Information Security in Companies: How to Meet the Need for Threat Information': in Dunn Cavelty, M., Mauer, V. & Krishna-Hensel, S.F. (eds), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot: Ashgate.

VeneKlasen, Lisa and Valerie Miller (2002) '*Power and empowerment*' PLA Notes 43: 39-41.

REFERENCES

[1] Several governments have released or updated cyber-security or cyber-defence strategies in the last several years. See http://www.ccdcoe.org/328.html for a good overview.

[2] The most frequently listed critical infrastructure sectors are: banking and finance, government services, telecommunication and information and communication technologies, emergency and rescue services, energy and electricity, health services, transportation, logistics and distribution, and water supply.

[3] The 2007 Estonia case refers to a series of cyber-attacks on Estonian digital infrastructure in the aftermath of the removal of a statue of a World War II-era Soviet soldier from a park.

[4] Due to space constraints, it cannot be covered at much length in this paper.

UI Occasional papers

WOULD YOU LIKE TO KNOW MORE ABOUT UI?

The Swedish Institute of International Affairs (UI) is an independent platform for research and information on foreign affairs and international relations.

The institute's experts include researchers and analysts specialized in the field of international affairs. While maintaining a broad perspective, research at UI focuses on unbiased scientific analysis of foreign and security policy issues of special relevance to Sweden. UI as an organization does not take a stand on policy issues.

The UI research department produces a number of publications to facilitate engagement with policy and research communities in Sweden and beyond. Each type of publication is subject to an in-house planning and approval process including quality control. UI Occasional Papers are reviewed by senior staff at the institute. They solely reflect the view of the author(s).

Please contact our customer service, or visit our website: www.ui.se, where you will find up-to-date information on activities at the Swedish Institute of International Affairs (UI). Here you can also book event tickets, become a member, buy copies of our magazines, and access research publications. Also, join us on Facebook! You can get in touch with us through email: **info@ui.se** or **+46-8-511 768 05**

SWEDISH INSTITUTE OF INTERNATIONAL AFFAIRS
Visiting Adress: Drottning Kristinas väg 37, Stockholm
Postal Adress: Box 27 035, 102 51 Stockholm
Phone: +46 8 511 768 05 Fax: + 46 8 511 768 99
Homepage: www.ui.se