Center for Security Studies

STRATEGIC TRENDS 2015

Key Developments in Global Affairs

Editors: Oliver Thränert, Martin Zapfe

Series Editor: Andreas Wenger

Authors: Myriam Dunn Cavelty, Jonas Grätz, Michael Haas, Prem Mahadevan, Martin Zapfe

CSS ETH Zurich

ETH zürich

STRATEGIC TRENDS 2015 is also electronically available at:
www.css.ethz.ch

Editors STRATEGIC TRENDS 2015: Oliver Thränert, Martin Zapfe
Series Editor STRATEGIC TRENDS: Andreas Wenger

Contact:
Center for Security Studies
ETH Zurich
Haldeneggsteig 4, IFW
CH-8092 Zurich
Switzerland

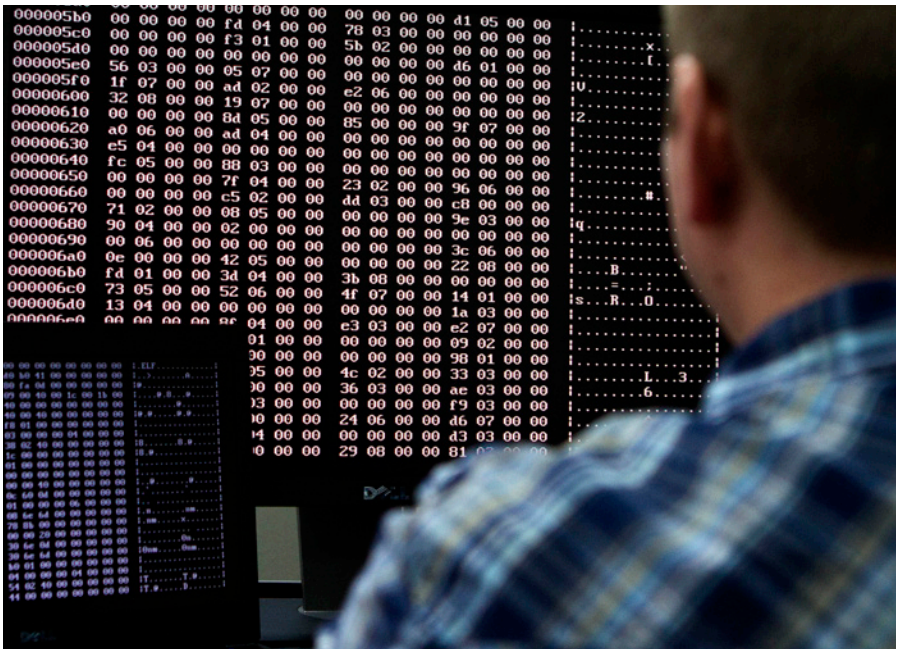
ISSN 1664-0667
ISBN 978-3-905696-48-6

CHAPTER 5

The normalization of cyber-international relations

Myriam Dunn Cavelty

We have arrived in an age of mega-hacks, in which high-impact and high-attention cyberincidents are becoming the new normal. The increase in strategically consequential, targeted cyberincidents is met with intensified efforts to reduce the risk of cyberconflict through norm-building, mainly geared towards creating deterrent effects at the state level. While these new developments have an overall stabilizing effect on cyber-international relations, the narrow focus on destructive cyberattacks and on state-to-state relations is creating unintended security-reducing side-effects.



An analyst looks at code in the malware lab of a cyber security defense lab at the Idaho National Laboratory in Idaho Falls, Idaho, 29 September 2011.

For half a decade, cyberincidents, both big and small, have made the news almost daily. The fact that insecurity in and through the cyberdomain has come to dominate political discussions is not a trend – it is old news. Nevertheless, something has subtly changed in the last few years: There is an increasing sense of unease about the escalatory potential of cyberconflict, mainly fueled by the certainty that more and more states are using cyberspace to achieve strategic ends. As a result, the traditional world of states is more actively seeking to stabilize political interaction in and through cyberspace by a variety of means. Overall, cyberspace has been upgraded to a strategic domain whose development is no longer left to non-state actors.

This chapter focuses on the efforts of states to pacify cyberspace. It explores both, the causes of this trend as well as wanted and unwanted consequences of this gradual normalization of cyber-international relations. Despite big differences between traditional security problems and the newer issues of cyberspace, states are using traditional tools of diplomacy and statecraft, shaped and tested during the Cold War, to develop norms. On the one hand, this stands in contrast to two major truisms of our age: that states have no power in the virtual realm and that traditional state response strategies are useless because the cyberdomain is too different. Since the cyberdomain is not a natural environment that develops beyond human control, it is almost entirely malleable. In other words, traditional response strategies and rules of conduct can be made to apply – at least in part. On the other hand, a focus on state-to-state relations and a focus on cyberattacks with destructive effects leaves two major issues untouched: first, how to extend norms, understood as shared expectations about appropriate behavior held by a community of actors, to non-state actors (both, as threat actors and security providers); and second, how to deal with large-scale cyberexploitation, or activities that are not destructive, but are used to extract data or to prepare for potential future 'cyberwar'. This omission leads to paradoxical effects: Even though more stability for state interaction is created, other state actions are, directly and indirectly, to blame for making both, the virtual but also, by implication, the real world rather less than more secure.

This chapter has three sections. The first discusses two developments in cyber-in-security. The first is about the 'normalization' of cyberconflict and the second about targeted attacks. Both trends give the impression that aggression in the virtual space has destabilizing effects and that there

is a high risk of escalation. A second section describes the attempts between states to stabilize interaction in cyberspace as a result of these insecurities and shows how norm-building is used to attempt cyberspecific deterrence. The third describes intended and unintended effects of these stabilization efforts, pointing to the main sources of tension. In conclusion, the chapter shows that the current stabilization and normalization processes are doomed to fail, unless the underlying issues are recognized and tackled.

Two trends in cyberaggression

To understand why states are seeking to stabilize cyber-international relations more actively nowadays, it is necessary to comprehend perceptions and realities of cyber-in-security. Two developments in cyberaggression stand out: The first is a shift in focus away from theoretical 'doomsday' cyberattack scenarios towards the reality of cyberaggression in conflict situations, which concerns both state and non-state actors. The reason for this shift is the 'normalization' of low-level cyberconflict as an add-on element to political disputes or conflicts. The second is a shift of attention from random occurrences to specifically targeted attacks. On the one hand, we have seen an increase in so-called 'mega-hacks' – successful data breaches in high-level economic or political targets. On the other hand, the focus of the debate is now on so-called advanced persistent threats, APTs, malware that is quite sophisticated and often written for a specific purpose or target. Both, mega-hacks and APTs, are signs of the increasing maturity of aggression and the professionalization of attackers. In combination, they point to the increasing involvement of states in cyberaggression.

From theoretical doomsday scenarios to low-level cyberconflict

The two strategic key concerns with regards to cyberspace are low entry costs for disruptive 'cyberweapons' and the high vulnerability of critical infrastructures, which are increasingly dependent on cyberspace for a variety of information management, communications, and control functions. This dependency, and interdependency, has a strong national security component, since information infrastructure supports and enables crucial services for the functioning of economy, government, military, and society overall. As a result, for years, the greatest threat in the virtual realm, discussed in strategic circles, has been a deadly destructive cyberattack out of the blue that would bring a country to its knees within seconds.

Even though the term 'cyberwar' is still used frequently and

Low-level cyberconflict / cybermobilization

Incident	Description	Actors
Estonia (2007)	• 3 week long wave of Cyberattacks accompanying riots in Estonia sparked by the removal of a Red Army soldier statue	• Patriotic (pro-Russian) hackers • No proof of state involvement – but also failure/ unwillingness to stop the attacks
Georgia (2008)	• Cyberattacks accompanying five-day international military conflict between Georgia and Russia	• Russian Patriotic Hackers • Russian Business Network (Criminal Internet Service Provider) • No proof of state involvement, but also failure/ unwillingness to stop the attacks
Ukraine (2013–)	• Cyberattacks accompanying the Russo-Ukrainian crisis	• Cyber Berkut (and other pro-Ukrainian hacktivist group) • Russian Patriotic Hackers • Paid cyber trolls
North – South Korea (2013)	• Cyberattacks accompanying the heightened crisis	• The New Romanic Cyber Army / The Who Is Team (hacker groups, claimed responsibility • North Korea (?)
Gaza (2014)	• Cyberattacks accompanying 'Operation Protective Edge'	• Pro-Palestinian actors (Anonymous, Hamas, Syrian Electronic Army, Iran Cyber Army) • No proof of state involvement

indiscriminately for any kind of cyberaggression, and doomsday scenarios continue to be referenced both, in policy circles and in the media, the larger attention of most experts has shifted to the political and strategic implications of low-level cyberconflict or cybermobilization. This shift occurs as strategic cyberwar or cyberterrorism for that matter – understood as stand-alone, out-of-the-blue cyberattacks against civilian infrastructure – is considered highly unlikely among experts, due to practical and strategic reasons since it is very hard to control the effects of cyberweapons and make them last long enough to serve a long-term strategic purpose. In contrast, low-level cyberconflict – or cybermobilization – occurs as an

Methods	Targets	Impact
• Distributed Denial-of-Service (DDoS) attacks, using botnets • Website defacements (Russian propaganda)	• Websites of Parliament, Prime Minister and President • Websites of Foreign Ministry, Ministry of Justice • Estonian Daily newspaper and broadcasters • Hansabank	• Very low primary impact (Websites unavailable, economic damage • Huge secondary impact: has become a signature event to prove how dangerous cyberconflict is
• DDoS-attacks • Website defacements	• Websites of the President of Georgia • Georgian Governmental Websites • Georgian Newssites • Russian Newssites • Georgian Banks	• Very low direct impact, also because Georgia is not heavily dependent on IT-infrastructure • Another signature event for 'cyberwar'
• DDoS-attacks • Website defacements • Data dumps • Disinformation and propaganda campaigns • Disruptions and infiltration of internet and mobile phone traffic	• Government websites and prominent media outlets telecommunications • Internet traffic	• Low effect on the conflict itself
• DDoS-attacks • Malware that wipes master boot records • Defacement of websites	• South Korean banks and broadcasting companies	• Relatively low effect on long-standing conflict • Has heightened attention on North Korean cyber-capabilities
• DDoS-attacks on Israeli targets • Website defacement • Data dumps • Spear-phishing	• Israeli websites	• Very low effect on the conflict itself

add-on to 'normal' conflict or political disputes. It mainly consists of information dissemination activities and hacktivism, a portmanteau word that combines 'hacking' and 'activism', in which different actors try to manipulate the public infosphere or in which non-state actors side with one of the conflict parties use cyberspace for disruptive activities.

While strategic cyberwar is about (very) low-probability, (very) high-impact events, low-level cyberconflict is about medium- to high-probability, low- to medium-impact events. There have been no known instances of the first case, but many of the second.

These incidents demonstrate that it has become routine for non-state

actors to try and influence the larger infosphere before or during conflicts/disputes. Cyberspace facilitates the proliferation, and use, of capabilities needed for information campaigns, and no hacking skills are required to obtain and operate disruptive malware like Distributed Denial-of-Service (DDoS) tools for political ends. Events of this kind with the biggest impact are those like Estonia in 2007, in which state-involvement is suspected but relatively hard to prove, or Georgia in 2008, in which there were clear attempts to dominate the public infosphere. That said, easy-to-use tools for DDoS attacks, for example, which always gain much attention because they produce visible effects, have relatively little lasting effect on the overall conflict. In other words, this type of cyberaggression is defined by low barriers to entry but also low direct impact – unless we take into consideration the secondary, and often delayed, effects on the broader strategic-political context, which is fundamentally shaped by overblown reactions to relatively low-impact events, such as the attacks on Estonia.

Targeted attacks: hacktivist campaigns and APTs

The second development is a shift away in focus from cyberthreats that attempt to infect or affect as many machines as possible – as done by most viruses, botnet malware, or spam mail servers – towards smart targeted attacks that use tools to get specific information or to disrupt a specific system. What is causing this shift, is the professionalization of the cybercrime market and more state involvement in cyberexploitation activities. That said, this type of targeting behavior is not entirely new: The period between 2008 and 2012 was dominated by headlines about targeted hacktivism. During that time, the hacker collective Anonymous successfully engaged in politically motivated, digital vigilante campaigns either to humiliate high-visibility targets by DDoS attacks or to point out cases that constituted interferences with freedom of information and freedom of speech, often by making secret information available. In comparison to the hacktivism during times of conflict, this type selects targets depending on a feeling of collective anger or outrage without the context of a conflict.

The fact that this type of hacktivism is viewed through the lens of national security at all is due to the nature of some of the targets that were chosen. Financial institutions, which were targeted in Operation Payback in 2010, for example, are considered 'critical infrastructures' by all states, so that cyberattacks against them have to be taken seriously by security actors.

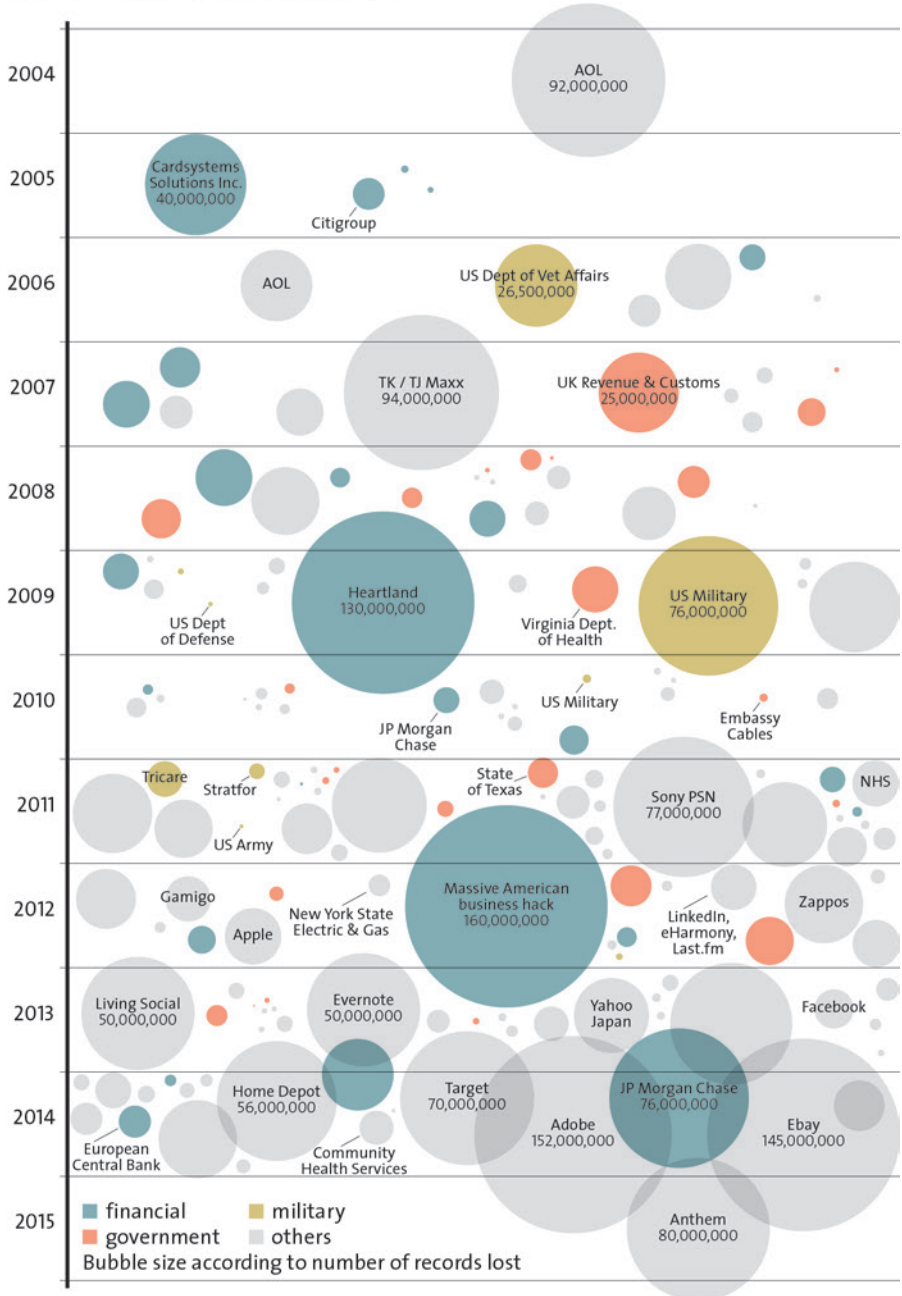
This also explains why incidents such as DDoS attacks, which are technically simple and harmless in terms of consequences, are often designated 'national security' issues. Furthermore, because some hacktivist campaigns aim to 'set information free', they clash with the state's prerogative to classify information and keep it secret. In 2011, hacktivist groups with higher technical proficiency went after high-level and security-designated targets such as the cybersecurity contractor HBGary Federal, the global intelligence company situated in the US Stratfor, or the CIA website. Several governments reacted with show trials of hackers and harshly prosecuted several of the individuals responsible for the above break-ins. Clear attribution was possible, due to an insider who helped the FBI and other security agencies to collect evidence against members of this group as part of a plea deal.

The steep decline in spectacular Anonymous-led hacktivist campaigns in recent years is likely due to the rather severe public punishment of misdeeds and a growing realization that cyberspace might not be quite as anonymous as assumed among hobby hackers. However, even though digital vigilantism and their showcase hacks have become less prominent, so-called 'Mega-Hacks' have exploded in numbers as it is shown in Figure 1. This form of cybercrime focuses on stealing massive amounts of (badly) secured data, like costumer records, credit card information, or e-mails. Costs such as forensic expenses, fines, legal fees, re-organization, reputational damage, and class-action lawsuits exceeded USD 100 million in several cases. Breaches and data theft at Boeing, the US Transportation Command, the US Army Corps of Engineers, and the US Investigations Services once again established a clear link to national security.

The motivation behind these hacks seems to be mainly criminal, but some seem at least partially politically motivated, making a clear categorization difficult. In some cases, state-involvement is suspected, like in the recent Sony hack, which was attributed to North Korea by the FBI. However, most of the data breaches and subsequent data dumps do not require advanced hacking skills at all, which shows how poor the standards of information security in large parts of the economy and government are.

There are targeted attacks of a different league, however, called Advanced Persistent Threats, APTs. APTs are stealthy and continuous cyberoperations targeting a specific entity's information or functionality. They are advanced because the malware that is

Selected 'Mega-Hacks' since 2004



Sources: DataBreaches.net; IdTheftCentre; informationisbeautiful.net

used is sophisticated. They are persistent because there is constant monitoring of the activity of the malware and often constant extraction of data. And they are called 'threats', in line with information security vocabulary, since they are orchestrated by a human actor. Granted, the percentage of APTs in the overall malware environment is very small – a maximum of three per cent, according to some analysts – but due to their potentially considerable effects, they have gained a lot of attention in recent years.

Also, there is no question that APTs embody the involvement of states in cyberspace operations. While there are low barriers to entry for patriotic and activist hackers, the barriers to entry are substantially higher when it comes to cybertools used to achieve strategic objectives. To achieve controlled effect, it is necessary to have the capacity to know and then exploit the vulnerabilities, parts of the code that can be exploited, in specific systems around the world. Overall, the insecurity of the information infrastructure is endemic: So-called vulnerabilities abound, and many of them are either not (yet) known, are known just to a few, or are known, but nobody has an incentive to patch them. Depending on what can be done with them, some vulnerabilities have high strategic or monetary value and are sold for as much as USD 200,000 to 300,000, often to national intelligence actors.

Once knowledge of an unpatched vulnerability has been gained, malware to exploit that vulnerability can be written. At minimum, this requires technical brainpower, labs that duplicate the target environment for testing, and a lot of time. In addition, many APTs are most likely inserted into the target systems by on-site personnel, including insiders. Most APTs remain undetected for years and gather large amounts of data during that time. Once malware has been inserted, it can also be modified in its behavior later; for example, to start deleting information or to tamper with other data functions. As a result, there are currently no good defenses against APTs. The usual tools like virus scanners and firewalls certainly do not work, but even air-gapped systems that are not connected to the internet can be infected, for example through a human agent.

Deterrence effects through international cybersecurity norms

The two cyber-in-security trends, normalization of low-level cyberconflict on the one hand and increasing state involvement on the other, demonstrate that the tools for and use of aggression have matured considerably in the last few years. The overall

feeling in many strategic circles, partially supported by statistics, is that the problem has gotten worse, both, in quantity as well as quality. Many experts call APTs cyberweapons and regard the build-up of capabilities by state actors as part of an arms race in cyberspace. The uncertainty about the intentions of other states and the practical inability to know whether such capabilities are used for offense or defense, lead to heightened feelings of insecurity and, in a classical security-dilemma fashion, to high incentives for building up (offensive) cyberwar capabilities and cybercommand units.

The further militarization of the virtual realm seems unstoppable at this point. However, the high feelings of insecurity have also led to higher incentives for states to control the risk of escalation and conflict. As a result, the number of ministerial meetings and conferences has increased substantially, and the first norms aiming to curb aggression in and through cyberspace are emerging. In this section, three types of developments are described that are leading to more stability in international relations through norm-building. The first concerns the establishment of transparency and confidence-building measures, TCBMs, for the use of information and communication technologies in conflict. The second occurs in the field of international law, where rules of warfare in and through cyberspace are being established. The third is the attempt to make deterrence apply to cyberspace, which builds on both of the other developments.

Transparency and Confidence-Building Measures

The notion of Transparency and Confidence-Building Measures (TCBMs) in international relations emerged from attempts by the Cold War superpowers to lower the risk of nuclear war. Based on the experience that uncertainty about the intentions of a rival has great escalatory potential, these measures aimed to create more overall transparency, enhance the mechanisms for early warning and predictability of action by enhancing one's knowledge of the capabilities of the other and by institutionalizing lines and forms of communication.

In the virtual realm, there is a high risk of misperception and therefore escalation, mainly, because hostile actions are notoriously hard to attribute and because almost all 'cyberweapons'are of dual-use nature. Actions in cyberspace leave ample room for speculation as to underlying intentions and purposes, and it is easy for third parties to start false-flag operations to provoke a cyberconflict

that suits their interests. Since classical arms control initiatives based on regulating technical capacities do not work in this realm – cyberattacks rely on knowledge about computer code and organizational routines that cannot be prohibited and/or controlled at any sensible cost – the existing proposals for stabilizing this environment are about TCBMs, with a main focus on transparency measures.

After years of failed attempts to come to any kind of multilateral agreement, the Organization for Security and Cooperation in Europe, OSCE, managed to establish an 'Initial Set of OSCE CBMs to Reduce the Risks of Conflict Stemming from the Use of ICTs' in December 2013. The CBMs focus mainly on transparency measures to allow for exchange of information and communication on several levels, all voluntary. Granted, since no notification or observation measures are included in the OSCE agreement, it is little more than an expression of goodwill between participating states at the moment. However, the document has an important psychological effect in that it proves that consensus is at last possible in international cybersecurity. Furthermore, a second set of CBMs is being discussed. The existing agreement also serves as a platform for engaging other stakeholders, such as civil society, academia and the private sector.

At the same time, dialogs have been taking place between states and between states and other relevant stakeholders, all of them aimed at building better understanding, trust, and confidence between the parties and at establishing joint information mechanisms to avoid escalation to armed conflict. In sum, even though the results of these processes are a far cry from what would be needed to fully stabilize cyber-international relations, reaching even minor agreements in this area is a considerable step forward, given how ideological differences have acted as fundamental stumbling blocks for years.

The law of cyberwar

Beyond transparency and confidence building measures, the applicability of international law to the cyberdomain has been discussed for years. In 2013, finally, a consensus emerged among several states, and at the UN, in the EU, and in NATO, that International Humanitarian Law, IHL, fully applies in cyberoperations. In parallel, the applicability of state sovereignty and the international norms and principles that flow from sovereignty were also confirmed by several intergovernmental bodies. The most important questions with regard to *jus ad bellum*, i.e., when a cyberattack would be considered an armed attack by another state and how to

react in that case, are discussed in the influential 'Tallinn Manual on the International Law Applicable to Cyber Warfare', which was written by a group of international legal experts in a three-year consultation process and published in 2013.

The Tallinn Manual, which sets out 95 black-letter rules governing cyberconflicts, states that any cyberoperation by one state that causes meaningful damage or injuries to another can be considered an 'international armed conflict'. This is extended to non-state actors: an international armed conflict exists whenever a state is in 'overall control' of a group that launches a substantial cyberattack against another state. In most cases, therefore, IHL will apply to cyberoperations involving a non-state group only when the operations are one component of the group's traditional hostilities or take place under the direction of a state. Clearly, most hacktivist attacks do not fall under this definition because they do not create severe effects and because proving a link to the state is very difficult in many cases. Indeed, the biggest issue in this whole debate is whether a cyberattack could actually be attributed to the perpetrator with enough certainty to make the logic of 'armed attack' apply. Because of how information is transported through cyberspace and because of the potential time lag between the effect of a 'cyberweapon' and the actual moment when such an APT is inserted into a network, there often is a serious attribution problem.

Making the logic of deterrence work

Attribution is also the biggest impediment against making traditional strategic concepts such as deterrence, especially deterrence by punishment, work. However, there are clear signs that the US is working systematically to build a specific deterrence regime for cyberspace, which encompasses both, deterrence by denial and deterrence by punishment. The considerable involvement of US officials in many of the international cybersecurity governance processes is linked to its strategic interest in shaping international norms for behavior in cyberspace, which will create more certainty about the costs of a cyberattack.

Traditionally, three interrelated components, the 'three Cs', are considered the necessary elements of successful deterrence: capability, credibility, and communication. A defender needs to have the necessary capabilities to inflict harm upon an attacker after being attacked (punishment), as well as the capabilities to defend against an attack or to deny either the weapons technology or the success of an attack (denial). Second, the challenger needs to believe that the defender is willing

and able to execute a retaliatory strike or is indeed able to defend or deny. Third, the defender should communicate to the challenger what to expect if he chooses to attack so that risk calculations can be made.

The capability to attack in cyberdeterrence consists of the knowledge of the vulnerabilities in an opponent's systems and the ability to exploit them. In this domain, in which 'weapons' are quasi-invisible, capability can be demonstrated indirectly, e.g., through institutionalization of cyberwar capacities in the form of cybercommands or directly by allowing attribution of sophisticated cyberattacks. For many observers, Stuxnet, the worm that sabotaged the Iranian atomic program, is such a case: Even though the US government has never officially confirmed its involvement, its key role is considered a fact in the international community and thereby serves to demonstrate and communicate the US has the capability and willingness to use an advanced cyberweapon against an adversary.

The credibility of one's ability to punish an attacker is linked to the possibility of attribution. True technical attribution in cyberspace is often impossible, especially in the case of APTs. However, the interesting trend that has become discernible is that there are in fact many cases of attribution in cases of cyberaggression, the latest being the identification of North Korea as the main perpetrator behind the Sony Hacks of 2014 by the US government. There are several aspects of importance: One, the norm is to apply the *cui bono* logic – to whose benefit – as the next best thing to true attribution, justified by the fact that cyberaggression hardly ever takes place in a strategic vacuum. Two, attribution is linked to the ability to fuse many sources of intelligence, some of which might be linked to APTs that are inside a potential enemy's networks already. Three, credibility is linked to the emerging norms in cyberconflict. By establishing clarity regarding what can be considered an armed attack in cyberspace and when escalation to another domain (i.e., conventional countermeasures) is possible, the costs of an attack become clear, and a more credible threat to escalate can be made.

The capability to defend or deny in cyberdeterrence, on the other hand, is linked to active and passive defensive IT-security measures and the resilience of systems. Resilience signifies the ability of systems, by means oftechnical, social, and political aspects, to deal with interruptions or crisis without breaking down. There are additional elements at play here,

such as being able to identify and to patch the biggest vulnerabilities in critical infrastructures. Establishing credibility in this domain is very difficult, considering the near-constant reporting of breaches in all kinds of networks. However, cybersecurity, cyberdefense, and resilience strategies can serve as declaratory elements to communicate institutional capabilities, for both, punishment and denial, and intentions. The case of five Chinese military officers indicted by a US court can be seen as such a declaratory action too: It signals that state actors are not immune from the law and establishes fairly clear red lines against cyberespionage for economic advantage.

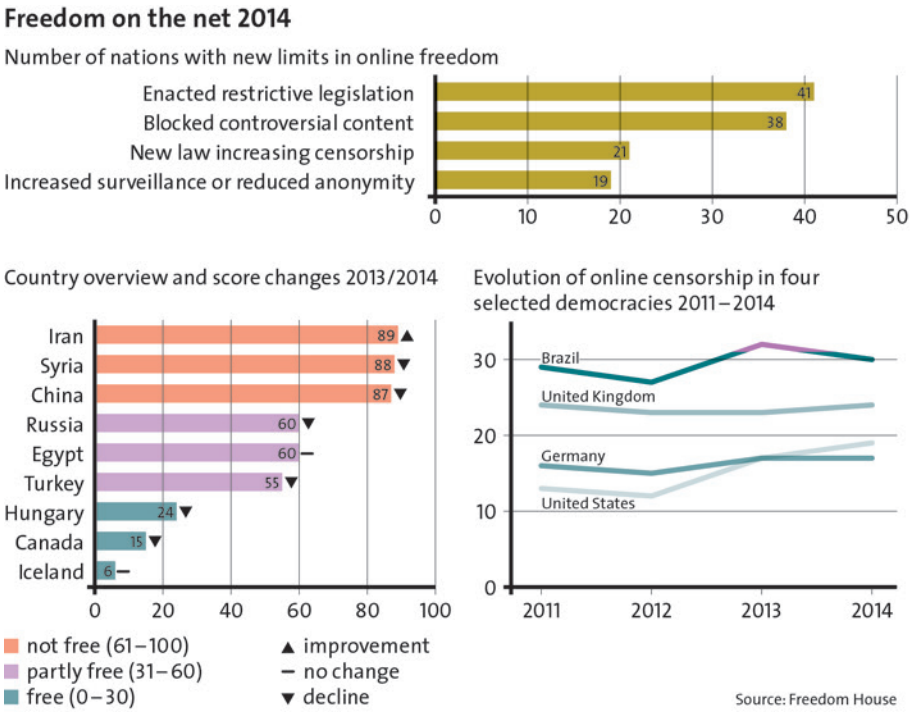
The side-effects of normalization

Given the resources that states have at their disposal, they have been singled out as most dangerous threat actors in this security domain. On the one hand, the trend of stabilizing political interactions in and through cyberspace thus has positive effects by reducing the risk of escalation. Still, the stabilization of cyber-international relations has been a slow process, and many observers are highly critical of the actual effects, given how easily rules can be altered and agreements broken.

Overall, it is too early to make conclusive statements about how effective the slowly emerging cybersecurity governance complex will be in the future in enhancing security. However, two related side-effects are already clearly discernible: The first is related to the focus of states on states as most dangerous actors, which causes more resources to be spent on pacifying state-to-state relations and fewer efforts to be expended counteracting malicious non-state actors and creating greater cybersecurity together with private actors. The second side-effect concerns the focus of the emerging cybersecurity governance complex on cyberattacks.

States, power, and cyberspace

As states are showing their willingness to place security needs above any other need when looking at cyberrelations, a widespread 'cyberutopia', which has dominated large parts of the information age, is coming to an end. For years, pundits have assured themselves of the powerlessness of states in the virtual realm and have shaken their heads at the attempts to respond with traditional tools to various policy issues concerning cyberspace. However, they had to realize that cyberspace may be different, but that the rules of the game can still be changed – by states. Concepts, such as 'Cyber-Westphalia', which lauds the benefits of order in the virtual space, based on the norms of



sovereignty and power concentration in the hands of states, have guided the actions of the international community in the last few years. While international talks have increased in intensity and numbers, this has also meant more control of 'national' cyberspace – which always equals more control over information flows. Authoritarian governments are embracing this growing 'cybersovereignty' movement to further consolidate their power. In democratic states, there is more government surveillance and more censorship than ever before.

But while there are many positive signs of more stability and normalization in the international realm because of this recent focus on state-to-state relations, this seizing of power by states is not uncontested. Because cyberspace is a realm used by different actors for highly diverse activities, the security-seeking actions by states often directly clash with other uses and conceptions of cyberspace. This causes considerable resistance to the actions of governments, with high costs for all sides. In particular, there are problems associated with

the empowerment of intelligence and military establishments in matters of cybersecurity. The military accumulation of cybercapabilities may be outpacing civilian comprehension and control. Similar problems hold true for intelligence agencies: While they may have the budget and technological resources that are best suited to respond to cyberthreats, their role also elicits great public unease. Public disquiet over government surveillance and cyber capabilities could prove to be difficult for cybersecurity strategies in the future.

Cyberexploitation as destabilizer

The second side effect is the result of the very specific focus of cybersecurity norm-building on destructive cyberattacks. Normalization and stabilization efforts are geared towards a form of cyberaggression that could indeed be devastating, but that also has a low probability of occurrence. The biggest current issue, besides cybercrime, is cyberexploitation, which is done with the help of APTs: the world of intelligence communities, whose actions in home states are regulated by national law, but who are expected to act unfettered and without restraint in the international realm.

In that sense, the perennially insecure cyberspace is an Eldorado for actors who are interested in collecting data. The big problem in cyber-international relations is that continued cyberexploitation by certain state actor threatens to undermine any stability that can be created through norms. They 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. Edward Snowden's revelations in 2013 exposed that the NSA had bought and exploited vulnerabilities in current operating systems and hardware to inject malware into numerous strategically opportune points of the internet infrastructure. It is unknown, which computer systems have been compromised – but it is known that these backdoors or sleeper programs can be used for different purposes, as forsurveillance, espionage, and disruption, for example, and activated at any time. It has also been revealed that the US government spends large sums of money to crack existing encryption standards in the name of counterterrorism – and apparently has also actively exploited and contributed to vulnerabilities in widespread encryption systems.

The crux of the matter is that backdoors and unpatched vulnerabilities reduce the security of the entire system – for everyone. Strategic exploitation of vulnerabilities in computer systems and the weakening of

encryption standards have the potential to destroy trust and confidence in cyberspace overall, which would be a disaster from an economic perspective. Neither is there any guarantee that an intelligence actor who has acquired knowledge about an exploitable vulnerability, has full control over it and/or can keep it secret. Capabilities in cyberspace are a derivative of knowledge. Hence, they can just as well be identified and exploited by criminal hackers or even 'terrorists'. The OpenSSL Heartbleed bug that was exposed in 2014 is a case in point: there is evidence that the NSA knew about this flaw and kept it secret, in order to be able to exploit it for intelligence purposes. Leaving crucial vulnerabilities open deliberately will also nullify attempts to make deterrence logic work in cyberspace: If deterrence by punishment is not credibly linked to deterrence by denial, which ultimately requires a very active anti-vulnerability policy, it will not be able to unfold any effect.

Conclusion

States are back in cyberspace – and they are rapidly expanding their power in an attempt to gain more security. The trend is to invest in state-to-state relations to normalize cyber-international relations, focusing mainly on transparency measures and attempts to create deterrence effects through norm-building. This is currently giving rise to hope for more stability, as the risk of escalation is reduced. Overall, then, a secure, safe, and open cyberspace is not possible without involvement and commitments of states. At the same time, states remain the biggest threats to stability. State practices linked to cyberexploitation are emerging as a major part of the problem, constantly creating more insecurity and, in fact, also hindering the removal of known insecurities.

It is clear from recent developments that we cannot have both, a strategically exploitable cyberspace full of vulnerabilities and a secure and resilient cyberspace. How, then, can this problem be overcome? Because cyberspace is shaped and used by many non-state actors, solutions are not to be found solely in the cooperation between states. Rather, a focus on a common issue of interest for all stakeholders interested in more security is needed. Computer vulnerabilities constitute such common ground. In other words, if the goal is a secure and resilient cyberspace, then then active efforts are required to reduce strategically exploitable vulnerabilities in cyberspace This is a compromise that some state actors need to make if they want the type of national security that extends to cyberspace. If such a compromise is not achieved,

the dilemma will remain: The quest for more national security will always mean less cybersecurity, which will always mean less national security because of vulnerabilities in critical infrastructures.