Working Paper
Research Division EU/Europe
Stiftung Wissenschaft und Politik
German Institute for International
and Security Affairs

Annegret Bendiek, Tobias Metzger

Deterrence theory in the cyber-century

Lessons from a state-of-the-art literature review

Ludwigkirchplatz 3−4
10719 Berlin
Phone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

Working Paper RD EU/Europe, 2015/ 02, May 2015
SWP Berlin

Table of Contents

List of Figures

List of Abbreviations

AA	German Federal Ministry of Foreign Affairs
BMI	German Federal Ministry of the Interior
BMVg	German Federal Ministry of Defence
BSI	German Federal Office for Information Security
BW	Bundeswehr, German Federal Armed Forces
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team for the EU-institutions
cf.	compare
CI	Critical Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CRITIS/KRITIS	Critical Infrastructure
CSIS	Center for Strategic and International Studies
DDoS	Distributed Denial of Service
e.g.	for example
EDA	European Defence Agency
EEAS	European External Action Service
ENISA	European Network and Information Security Agency
EU	European Union
EWI	EastWest Institute
ICT	Information and Communication Technology
IP	Intellectual Property (also Internet Protocol, as in IP address
IT	Information Technology
LOAC	Law of Armed Conflict, also called International Humanitarian Law (IHL)
MAD	Mutually Assured Destruction
n.d.	no date
NATO	North Atlantic Treaty Organization
NCAZ	German National Cyber Response Centre
NCSR	German National Cyber Security Council
NIS	Network and Information Security
NIST	U.S. National Institute of Standards and Technology
NSA	U.S. National Security Agency
OSCE	Organisation for Security and Co-operation in Europe
SCADA	Supervisory Control and Data Acquisition
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
UN	United Nations
UN GGE	United Nations Group of Governmental Experts
UN GA	United Nations General Assembly
USA / U.S.	United States of America

Introduction

Cyberwar is regularly invoked in journalistic, academic and even political discourse. Yet, apart from the U.S.-Israeli Stuxnet attack on Iran's nuclear facilities in 2010, no cyberattack has ever caused large-scale physical damage. UK Labour last year urged their government to consider the "growing threat of cyberwarfare"[1] and former Defence Secretary Leon Panetta repeatedly warned of the lurking threat of a "cyber Pearl Harbour".[2] While the Stuxnet attack remains the only instance of severe physical damage inflicted via cyberspace, the Internet's increasing pervasiveness and national development of military units bear the risk of militarization. Connecting growing parts of the German industry, energy production and society to the Internet fosters economic growth, increases efficiency and, benefitting from the Internet's anonymity, furthers human rights. Nevertheless, U.S. think-tanker Jason Healey cautions that, as the Internet of Things spreads, "a cyberattack will destroy not only ones and zeros, but things made of steel and concrete. And when they break, people will die."[3]

To achieve restraint from attacks, deterrence theory has long been considered a valuable concept. While deterrence will remain an instrument in security policy – any consideration of deterrence theory must acknowledge that its limitation to the military, and more specifically the nuclear, domain is insufficient.[4] In line with this, various authors have discussed the extent to which deterrence theory is applicable to cyberspace. Their findings of appropriateness and limitations are a necessary starting point for policy-making recommendations. How do the criticisms of classical deterrence apply in this relatively new domain, and how does cyberdeterrence differ from its kinetic counterpart? Can offensive cyber capabilities be effective in deterring adversaries? Must kinetic retaliation be "on the table" for deterrence to succeed? Which changes are required for its implementation and where do key challenges lie?

Different from Gaycken and Martinelli, the concept of cyberdeterrence in the following is built on both deterrence of cyberattacks and deterrence by threatening cyberattacks, arguing that rather than being separate, they are different escalatory steps and conceptually cannot be separated.[5] The means of deterrence are part of an overall toolbox and discussing cyber separately would be similar to speaking, for instance, solely about deterrence effects of the navy or air force. The authors build upon Lawrence Freedman's types of deterrence: deterrence-by-retaliation and deterrence–by-denial; "narrow" vs. "broad"; "central" vs. "extended" and "immediate" vs. "general" deterrence. Addressing these question is essential for determining a deterrence strategy's effectiveness. In its study for the U.S. Air Force, RAND subsumes only questions of punishment as deterrence, while referring to all deterrence-by-denial mechanisms as "defence".[6] It suggests that deterrence-by-denial and deterrence-by-retaliation ought to be considered separately. Other authors see deterrence-by-denial as part of an "active defence system"[7], denying would-be-offenders opportunities and putting the defender in control[8], while we argue, to the contrary, that they are complimentary.

Threat perceptions play a central role both for developing an effective national strategy and for the purpose of applying deterrence theory. Understanding a country's or an organisation's threat assessment is crucial to understanding their strategic response. The nature of a threat, threat agents, the technical means used and the potential target are thus important. ENISA, the European Network and Information Security Agency, identifies six threat agents in national strategies, namely corporations, cybercriminals, employees, hacktivists, nation states and terrorists.[9] A NATO CCDCOE study adds state-sponsored agents as a seventh actor.[10] The German cybersecurity[11] strategy recogniz-

[1] Mason 2014

[2] Secretary of Defence Panetta 2012

[3] Jason Healey at SDA, Annual conference 2014, 31

[4] Schwarz 2005, 5-6

[5] Gaycken and Martinelli differentiate „cybered deterrence", as deterrence by cyber means, and "cyber deterrence", as deterrence of cyberattacks. Cf. Gaycken and Martellini 2013

[6] Cf. Libicki 2009, 7,8

[7] "Active" usually refers to measures such as missile defences, whereas passive defences are the modern equivalents of moats or bunkers.

[8] Cf. Guitton 2013, 30

[9] Cf. ENISA 2013, 2; The OSCE further specifies the vague term "cyberterrorism" to signify "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives", OSCE 2013, 16

[10] Cf. NATO CCDCOE n.d.

es these threats, noting that "[e]nsuring cyber security has thus turned into a central challenge for the state, business and society both at the national and international level."[12] To avert these threats, the strategy "mainly focuses on civilian approaches and measures" while "complimented by measures taken by the Bundeswehr to protect its capabilities … to make cyber security a part of Germany's preventive security strategy".[13] Together with the BMI, the Foreign (AA) and Defence (BMVg) Ministries complement German efforts in cyberdefence and cyberdiplomacy.

The BMVg, operating the CERT-Bundeswehr, has the primary responsibility to protect military operations and networks. Since mid-April 2012 it is known that the Bundeswehr does not solely rely on defence. In response to a Bundestag inquiry, it admitted to having developed an initial capacity to attack enemy networks since 2006.[14] While such capabilities – similar to submarines in maritime warfare – can only be used in attack scenarios, the Bundeswehr has not conducted or threatened any such operation, holding these capabilities available for emergencies.[15] It is most concerned about protecting its own networks, which appear much less secure after Stuxnet infected Iranian systems entirely disconnected from the Internet. Such incidents, for instance, led to a ban on USB-Sticks, CDs and other external hard drives in all Bundeswehr facilities.[16]

For deterrence to be effective in cyberspace, actors dealing with foreign and security policy can find useful reference points in the state-of-the-art literature on deterrence theory and cyberdeterrence.

In theory – Deterrence theory and cyberspace

Throughout the Cold War, deterrence theory was the preferred framework of analysis and of military doctrine to explain the influence of nuclear weapons, and to argue that nuclear powers, fearing the consequences, would not go to war with each other. Some authors have since applied the theoretical framework to cyberspace[17], as cyberdeterrence[18]. While both domains share characteristics, such as the offensive advantage, given the difficulty and costliness of defence[19], significant differences exist.

The emergence of deterrence in military theory dates back to the 1920s/30s when the first flight bombers were considered unstoppable by defensive measures. Then, strategists thought that large-scale attacks on one's cities could only be prevented, if the other side feared counter-attacks of similar or greater magnitude. The first nuclear bombs demonstrated a similar offensive advantage, and Bernard Brodie, in 1946 after having witnessed their destructiveness, was among the first to observe that "from now on [the military establishment's] chief purpose must be to avert [wars]".[20] Deterrence theory gained prominence and developed to its present state during the Cold War nuclear stand-off between the USA and the Soviet Union.

The term goes back to the Latin "dēterrere", meaning to "frighten from or away", and is defined as "to discourage and turn aside or restrain by fear".[21] "Deterrence is concerned with discouraging others from

[11] The lack of precise –, let alone, common – definitions gives rise to considerable confusion in the cyber domain, especially in the use of the term "cybersecurity".

[12] BMI 2011, 1

[13] BMI 2011, 5

[14] Cf. Fischer, Blank and Dernbach 2012

[15] Interview German BMVg Cyberdefence Official 2014

[16] Cf. Grunert 2013, 110

[17] Authoritative documents are inconsistent in spelling cyber terminology. We follow the "Oxford Dictionary for Scientific Writers and Editors" in that "terms in which the first word is 'cyber' are usually written as one word", Oxford Reference n.d.. To improve readability a hyphen is inserted to prevent double-consonants: i.e. "cyber-resilience".

[18] For in-depth accounts, see Knopf 2010; Geers 2010; Cilluffo, Cardash and Salmoiraghi 2012; and Gaycken and Martellini 2013

[19] See also Lieber 2014, 5, 96: Although such analyses are somewhat doubtful, there are calculations of offense being 132 times cheaper than defence, and of a $100 million high-end "cyber army" being able to overcome any U.S. cyberdefence, cf. Malone 2012 and cf. Chapman 2010

[20] Brodie 1946, 31 and cf. Freedman 2004, 9-11

[21] Search for "to deter", Oxford English Dictionary 2014

acting in ways that advantage them but harm you".[22] This definition highlights the two notions of deterrence, firstly the would-be-attacker's turning back discouraged by the other's defences, and secondly restraint for fear of retaliation. The threat of force by *'A'* and the voluntary restraint of *'B'* are central elements. It is important for the following sections to differentiate what deterrence is, and what it is not. As Freedman puts it: "strategies geared to coercing others to act in ways they might consider harmful but advantage you have been described as compellence or coercive diplomacy".[23] The main difference is that deterrence seeks to preserve the "status quo" and is limited to persuading someone not to do something, while compellence seeks to enforce a change, typically within a frame of urgency.

Deterrence requires two components: the expressed intention of *A* to defend an interest; as well as the ability to achieve the defence or the (perceived) certainty by *B* that interference with *A's* interest will be costly for the attacker, i.e. credibility. However, signalling – used to communicate both the interest to be defended and the threats to be implemented in case of non-compliance – is never straight forward.[24] Freedman stresses the possibility of *A* badly articulating or B misunderstanding the threat, thus rendering deterrence ineffective. The movie "Thirteen days", set during the Cuban Missile Crisis, contains a scene in which U.S. Defence Secretary McNamara angrily stops the Navy from firing blanks at Soviet ships. While the military considers this appropriate behaviour to enforce the naval blockade, McNamara's character says: "This is language: A new vocabulary, the likes of which the world has never seen. This is President Kennedy communicating with Secretary Khrushchev!"[25] Signalling or "brandishing"[26] of weapon capability can be very costly, as evident in Israel's military operations aimed at deterring future attacks. The ultimate aim is strategic deterrence, thus creating "internalised deterrence", no longer requiring explicit signalling.[27]

Robert Jervis describes an evolution of "three waves of deterrence": Firstly, Brodie's concept of deterrence to avert wars when only the West possessed deployable nuclear weapons; secondly, the rise of the Soviet Union as a nuclear power leading to a bipolar world evoking the question "if nuclear war couldn't be fought how could it be threatened?". At this stage second-strike capabilities deployable from submarines assured Mutually Assured Destruction (MAD), making it impossible to inflict sufficient damage to disarm an enemy, which would prevent retaliatory attacks. Game theory was used, by Powell[28] and others, to evaluate whether cost-benefit evaluations could still favour deterrence postures, issuing a "threat that leaves something to chance"[29] or threatening sanctions using limited (non-nuclear) strikes. U.S. State Secretary Dulles argued for deterrence of would-be-aggressors from a cost-efficiency perspective, calling it "the way to getting maximum protection at bearable cost".[30]

One of the inventors of deterrence theory in criminology, late 18th century philosopher Jeremy Bentham, assumes rational individuals capable of performing cost-benefit calculations prior to taking action. The third wave raised considerable doubts about this rational actor model, an important pillar of deterrence theory, arguing that groupthink, misperceptions and bureaucratic politics often overruled mere cost-benefit calculations. Rationality is subjective, and the challenge of deterrence signalling consists in identifying the opposing side's rationale.[31] Furthermore, cost-benefit calculations require clarity and predictability of sentencing and proportionality between punishment and violation.[32] Bentham, for example, observed that where arrest is unlikely, severe punishment can help keep up a criminal's expected cost of getting caught, but once punishment is perceived as disproportionate, it loses its effect.[33]

In line with the controversy of "rational" actions, signalling can be misunderstood given differences in culture or education. Furthermore, there are claims of fallacies in traditional deterrence theory's sole consideration of state actors.[34] Third-wave theorists Alexander George and Richard Smoke disapproved of the exaggerated role of the military vis-à-vis other foreign policy tools, especially positive inducements.[35] The rise of non-state actors, "rogue states" and "terrorists", brought a possible fourth wave. These actors, accord-

[22] Freedman 2004, 109
[23] Freedman 2004, 109
[24] Cf. Kaufmann 1958 as printed in Libicki 2009, 7
[25] Simpson 2013
[26] Cf. Libicki 2013
[27] Cf. Freedman 2004, 28-32
[28] Cf. Powell 2008
[29] Cf. Schelling 1966
[30] Dulles 1989 as quoted in Freedman 2004, 9
[31] Cf. Morgan 1977
[32] Cf. Freedman 2004, 7, 8, 49, 116. Bentham's collected works are available online, cf. Bentham 1838-1843
[33] Cf. Libicki 2009, 29
[34] Interview NATO Cybersecurity Official 2014
[35] Cf. George and Smoke 1974

ing to former U.S. President George W. Bush, are beyond containment by deterrence since they have no “nation or citizens to defend”, thus necessitating preemptive measures.[36] The limited space does not allow for an evaluation of the relationship between deterrence, pre-emption and prevention, this quote, however, demonstrates the importance of knowing one’s adversaries and adjusting deterrence strategies accordingly. Finally, theorists introduced the differentiation between interest-based and norms-based deterrence in the 1990s to overcome previous challenges. The former aims at deterring challengers of “hard” national interests, while the latter advocates less clear-cut norms. The arguments for pre-emptive interventions follow from the latter.[37] Freedman argues for norms-based deterrence to reinforce “certain values to the point where it is well understood that they must not be violated”.[38] Instead of pure benefit-maximisation, norms introduce a variable of “doing the right thing”, and the UN Group of Governmental Experts (GGE) on Cybersecurity recommends agreeing on such norms and rules on actions below the threshold of international conventions as confidence-building measures,[39] Confidence-building, a key instrument of the OSCE, can enhance trust among states and help reduce the risk of conflict by increasing predictability and reducing misperception.[40]

Deterrence-by-retaliation and deterrence-by-denial

To dissuade would-be-offenders from attacking, deterrence theory typically distinguishes two means: denial and retaliation.[41] In the original criminological context, Bentham describes deterrence-by-retaliation, or deterrence-by-punishment, as imposing the “significant likelihood of any culprit being apprehended, brought to trial, found guilty and then receiving a sentence … that will make an impression not only on their future behaviour but on the behaviour of others”.[42] Whether in a criminological or military setting, B is deterred from harming A’s interests because “whatever gains might be obtained would soon be outweighed through the imposition of intolerable pain”.[43] This was the core idea of nuclear deterrence until the 1970s when U.S. President Reagan’s “Strategic Defense Initiative” (SDI) introduced the notion that is was better “to protect than avenge”.[44] Reagan strengthened the deterrence-by-denial approach, also referred to as “denial-of-benefit”[45]. Deterrence-by-resistance and deterrence-by-resilience are two different approaches within this concept. Resilience is the ability to quickly restore the original shape after an attack, Quick recovery limits potential gains and can convince an opponent not to attack, if the cost of attacking becomes excessive. Both – resistance and resilience – are concerned with reducing a would-be-offender’s options, either by building unsurmountable defence structures or by ensuring quick recovery following an attack.

Freedman extends the distinction beyond, firstly, the denial versus retaliation debate[46]: He, secondly, introduces “narrow” versus “broad” deterrence, distinguishing whether a particular military operation (e.g. the use of nuclear missiles) or any type of attack is to be deterred; thirdly, “central” versus “extended”, thus including the protection of third-party allies in one’s deterrence demeanour; fourthly, “immediate” versus “general” deterrence, distinguishing between a crisis situation between known actors and non-state of emergency deterrence against unknown would-be-aggressors.

Many of the same elements apply regarding attacks through cyber means although with some limitations. Signalling, for one, faces comparable challenges, although further complicated by the multitude of actors, including non-state groups and individuals. Other challenges are entirely new: In deterrence-by-retaliation, credibility is difficult to establish since demonstrating cyberpower and retaliating immediately and repeatedly is problematic, as outlined below. Although the U.S. and NATO have emphasized their willingness to respond to cyberattacks at a time, place and by means (including kinetic) of their choosing, there can hardly be automaticity in response. The similarity of nation-state and criminal cyberattacks requires time-consuming and costly forensics and close coordination between law enforcement and the mili-

[36] Bush 2002 as quoted in Freedman 2004, 24

[37] Cf. Freedman 2004, 80-88

[38] Freedman 2004, 4

[39] Cf. Stevens 2012, 156 and see: Maurer 2011

[40] Cf. Markoff 2014

[41] For the first debates, refer to Snyder 1958 and Snyder 1961

[42] Freedman 2004, 60, 61

[43] Freedman 2004, 15

[44] Freedman 2004, 19

[45] Cf. Davì 2010

[46] Cf. Freedman 2004, 32-42

tary. As for the U.S., Germany and other established powers, the reluctance to admit to its development of offensive capabilities, and to strategically discuss their legality, creates opaqueness and significant grey areas. Given the offensive advantage, the number of attackers using cheap, readily available tools will continuously rise, empowering non-established powers such as Iran, North Korea or even Daesh/IS. Reversing this trend requires getting serious about agreeing on international norms and improving both defences, especially employees' and citizens' "cyber-hygiene", and about enforcement. Lack of clarity and impunity for attackers is a major roadblock for effective deterrence.

In practice – Suitability of cyber: lessons and implications

The U.S. Army analysis that "[f]undamentally, there is no difference between deterrence in the cyber domain than in any other domain"[47] is flawed in at least three regards: First, cross-border differences in law enforcement and legal practice as well as unwillingness to cooperate allow attackers to act with impunity, diminishing the deterrent's credibility. Second, since "cyberweapons" rely largely on previously unknown, so called zero-day, vulnerabilities and cannot be displayed prior to their use, it is difficult to demonstrate power. Third, deterrence-by-denial differs greatly, since in cyber "you have to work from the assumption that your networks are already compromised"[48], meaning deterrence is constantly failing. In the nuclear context, all intrusions must be deterred, and a single instance of failed deterrence could mean the use of nuclear warheads and large-scale loss of life. Fourth, different from nuclear confrontation, uncertainty arises from the multitude of actors which threaten harm to one's systems and from the difficulty of quickly attributing an attack. Fearing unforeseen escalation, this may hinder immediate retaliation, especially when retaliating with kinetic strikes.

Ambiguously defined interests, misperceived signalling and uncertainty on how to demonstrate force and how to respond, hamper deterrence postures. Melissa Hathaway, former director of a classified high-level effort to establish a U.S. cyberdeterrence strategy, admitted that "we didn't even come close".[49] Contrary to classical deterrence, the private sector plays a crucial role resulting in problematic signalling. While being a useful frame of analysis, cyberdeterrence fails to satisfy any of Patrick Morgan's six elements[50] of classical deterrence theory, according to Stevens. First, there is no prevailing military conflict; second, rational choice models differ for non-state actors; third, the challenge of attribution complicates immediate retaliation; fourth, repeated retaliation and certainty of inflicting severe pain is hampered; fifth, the difficulty of demonstrating offensive capabilities lessens credibility; and sixth, a multitude of (non-state) actors constantly threatens stability, risking escalation.[51] Libicki aptly summarizes the core issues to be observed in national cybersecurity efforts: "The ambiguities of cyberdeterrence contrast starkly with the clarities of nuclear deterrence. In the Cold War nuclear realm, attribution of attack was not a problem; the prospect of battle damage was clear; the 1,000th bomb could be as powerful as the first; counterforce was possible; there were no third parties to worry about; private firms were not expected to defend themselves; any hostile nuclear use crossed an acknowledged threshold; no higher levels of war existed; and both sides always had a lot to lose."[52]

Key challenges: Credibility and capability to display and use force

Beyond technical issues – which are being addressed – deterrence-by-retaliation is a question of credibility and capability. Firstly, could governments effectively deploy cyberforce to respond to attacks, and should they use kinetic force – and if so under which circumstances – to react to cyberattacks, potentially risking escalation? Secondly, should there be stronger declara-

[47] Philbin 2013, 16

[48] Michael Daniel, Cybersecurity Coordinator of U.S. President Obama, at SDA, Evening debate: Critical infrastructure protection in the cyber-age 2014

[49] Hathaway 2010. On cyberdeterrence in U.S. strategy, see Stevens 2012, 154

[50] Cf. Morgan 2003, 8

[51] Cf. Stevens 2012, 152

[52] Libicki 2009, xvi

tions of cyberforce to signal one's ability?[53] For example, German offensive capabilities which were only revealed by a parliamentary inquiry, are not openly discussed or even used for deterrence signalling.

For deterrence-by-retaliation to work, the capacity to display force is crucial. Only verifiable tests and the demonstration of nuclear weaponry's destructive force during WWII convinced nations that future use must be feared. Similar demonstration of cyberpower[54] is unlikely because of the "one use only component"[55], meaning that any use reveals significant information necessary to defend against future attacks. Deterrence-by-retaliation requires a demonstration of force, but cyberattacks are rendered useless if vulnerabilities are closed.[56] Therein lies the danger of using cyberweapons and the difficulty of credible signalling. Signalling is complicated by the multitude of actors beyond the great powers, and including the private sector and individuals.[57] Willingness to retaliate requires unmistakable signalling on the interest to be defended. While offensive capabilities have been revealed, Germany has never publicly announced their existence or threatened adversaries with their use in response to attacks. France and the UK publicly announced offensive capabilities, and France stated its intent of becoming a cyberpower in its 2011 cyber doctrine[58], but both left it unknown when and how cyberweapons could be used.[59] The U.S., on the other hand, emphasized via the Pentagon that the "response to a cyber-incident or attack on the US would not necessarily be a cyber-response. All appropriate options would be on the table".[60]

Mutually assured destruction, equally, is out of the question, changing the cost-benefit calculation in favour of attack.[61] If the MAD principle does not apply, the consequences of retaliation are considerably less severe, reducing the inherent costs of an attack. This leads to an advantage for the party which strikes first, according to offence-defence theory, making attacks more likely.[62] While this suggests for other characteristics of offence-defence theory to apply – e.g. that an arms race ensues – the lacking ability to make quick and decisive victory changes the equation. If cyberattacks cannot disarm an opponent, what is the point of rushing into retaliation?[63] An attack may be stopped, but the attacker cannot be disarmed since cyberattacks can be conducted from third-party hardware, including internet cafés, unsecured wireless networks or infected computers, as part of a botnet.[64] Furthermore, the asymmetric nature of cyberspace is a common argument against retaliatory attacks against criminals or "cyber-terrorists". Deterrence fails if there is no valid target to strike back at. The less connected an adversary, the less vulnerable he is to retaliation with cyber means. Retaliation by kinetic means, on the other hand, bears the risk of incurring injuries or deaths where the initial attack did not.

Retaliation "requires not only breaking into sufficiently privileged levels, but also figuring out how to induce a system to fail and keep on failing".[65] The ability to induce superficial damage, which is quickly repaired, has no deterrent effect. Battle damage assessment (BDA) is difficult to predict ahead of an attack, as this depends on the other's technical and procedural resilience but also on chance – e.g. whether patches are installed, closing previously existing backdoors, some of which might have been intentionally created to allow attackers to bypass security measures.[66] The half-life of exploits creates a "use-it-or-lose-it dilemma".[67] While initial attacks allow for intensive intelligence work, repeated retaliation is costly, if not impossible, since it requires firstly rapid attribution and secondly immediate and continuous knowledge of the target system. Figure two puts this question in context.

[53] Cf. Goodman 2010

[54] For an analysis of cyberpower, see Nye 2011, chapter 5, and for its relevance on policy-making, see Sheldon 2011

[55] Cf. Libicki 2012, xv-xvii

[56] Cf. Libicki 2013, vii-viii

[57] Cf. Freedman 1998

[58] Cf. Lewis and Timlin 2011 and cf. Levin, Goodrick and Ilkina 2013, 25

[59] France: cf. Marchive 2013 and UK: cf. Blitz 2013

[60] BBC 2011

[61] Cf. van Evera 1998

[62] Cf. Quester 1977, 208

[63] Cf. Libicki 2009, 61-62

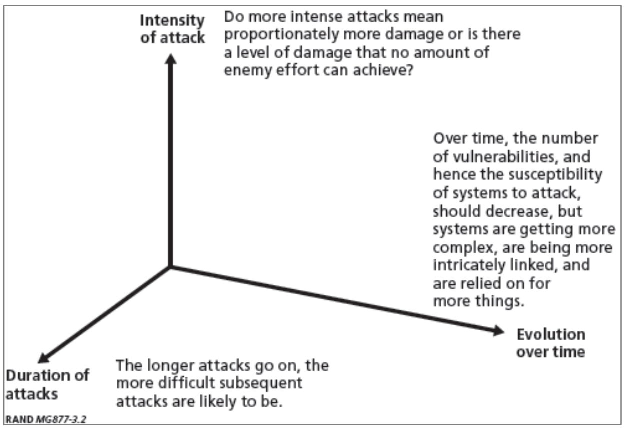
[64] Refer to Appendix A for technical definitions. For more detail, see Cheswick, Bellowin and Rubin 2003

[65] Libicki 2013, viii

[66] Cf. Cisco 2014, 12

[67] Libicki 2009, 58

Figure 1: Limits to retaliation in cyberspace[68]


Intensity of attack
Do more intense attacks mean proportionately more damage or is there a level of damage that no amount of enemy effort can achieve?
Over time, the number of vulnerabilities, and hence the susceptibility of systems to attack, should decrease, but systems are getting more complex, are being more intricately linked, and are relied on for more things.
Evolution over time
Duration of attacks
The longer attacks go on, the more difficult subsequent attacks are likely to be.
RAND MG877-3.2

Additionally, once the Stuxnet source code became available online, it revealed flaws in Siemens' operating system, thus enabling their use against other CI. Attackers "may risk handing over ammunition to the enemy as a blueprint for the latter to develop a cyber weapon of its own"[69] using reverse engineering.[70] Instead of taking advantage of such flaws and even buying such information off the black-market, governments must inform the manufacturer to rid systems of backdoors.[71] NSA exploitation of zero-day vulnerabilities and their purchasing with a 2015 budget of $25 million dollars[72] strengthens this business, and may open *Pandora's Box* encouraging others to follow suit rather than deterring them.[73]

How to deter? Deterrence-by-denial and deterrence-by-retaliation

In a cyberspace of easy targets, weak cross-border cooperation and diverging legislation the odds are tilted in favour of attackers. As RAND puts it, "if cyberattacks can be conducted with impunity, the attacker has little reason to stop."[74] Former White House advisor Richard Clarke admits that currently "we cannot deter other nations with our cyber weapons. Nor are we likely to be deterred from doing things that might provoke others into making a major cyber attack". According to him, deterrence requires getting "serious about deploying effective cyber defences for some key networks" and "since we have not even started to do that, deterrence theory … plays no significant role in stopping cyber war today". He demands a defensive triad of improving backbone network security, protecting critical infrastructures (CI) and improving the security of military networks and weapons.[75]

Determining the type of defence

For deterrence-by-denial to succeed, cost-benefit calculations of attackers must turn negative: "A strong defense deters an attack by convincing an attacker there will be no gains commensurate with the cost of attack".[76] Good defences make an attack less likely to succeed, add credibility to retaliatory measures, reduce the success rate of low-sophistication third-party attacks and make it easier to attribute attacks.[77] As an important differentiation, we note that deterrence-by-denial exists in the pre-event as defence, and in the post-event as resilience.[78] Bologna et al. urge to move from a "fortress" to a "resilience" approach[79], while a RAND study suggests "that, in this medium, the best defense is not necessarily a good offense; it is usually a good defense".[80] The importance of defence is evidenced in NATO's emphasis on cyber-hygiene. If a system is ridded of low-level disturbances, advanced threats are easier to identify and to counter.[81] "Honeypots", entirely sterile systems which capture malware and allow analysts to observe their behaviour in a vacuum, leverage this observation. Since not all targets vulnerable to cyberattacks can be protected with the same priority, risk management is crucial. Current cybersecurity strategies place strong emphasis on public awareness: Raising citizens' defences denies quick gains. This links into another dilemma: Today "national parliaments … hardly [participate] in the development of national cyber defence measures". "[B]oth the Bundestag and the European Parliament lack the scientific expertise … to perform these functions", thus

[68] Libicki 2009, 60
[69] Shaheen 2014, 78
[70] Cf. Rid 2012
[71] Freddy Dezeure, Head of CERT-EU at SDA, Evening debate - At a glance 2014
[72] Cf. Grossman 2014
[73] Cf. Reveron 2012, 155
[74] Libicki 2009, xvi
[75] Cf. Clarke and Knake 2012
[76] Philbin 2013, 2-4
[77] Cf. Libicki 2009, 73-74
[78] On pre- and post-event deterrence by denial, see Bowen 2004
[79] Cf. Bologna, Fasani and Martellini 2013
[80] Libicki 2009, 176
[81] Interview NATO Cybersecurity Official 2013

impeding information exchange between government, parliament, the public and the private sector.[82]

Another feature of cybersecurity strategies – especially that of the EU – is "strategic dependency management".[83] This includes all measures to secure key components of the supply chain by deciding which levels of strategic independence are required in industry R&D, manufacturing and maintenance of important IT components. It serves to minimize national risks[84], but often faces accusations of government protectionism. After the Snowden revelations risk management strategies led China to reduce their reliance on U.S. technology, e.g. deciding against Microsoft's Windows 8.[85] It also led to calls within Europe, e.g. by German Chancellor Merkel[86], for greater technological sovereignty from U.S. communication infrastructure. Such measures, while sensible in light of deterrence-by-denial, reverse the purpose of the global Internet. However, defensive measures, e.g. Iran's creation of parallel structures for a national network to prevent high-level cyberattacks, can be bypassed as evidenced in "Stuxnet", which infected the nuclear reactor's software via a USB-stick. Consequently, Germany has prohibited USB-sticks and other external devices in military installations. Difficulty of attribution and of retaliatory action is stated as necessitating these measures.[87]

While Germany uses offensive means to stop ongoing attacks[88] and works to strengthen cross-border criminal law enforcement, most actions can be seen from a deterrence-by-denial angle. The strong defence network of public and private Computer Emergency Response Teams (CERT) is one component, most importantly CERT-Bund for the federal government and Buerger-CERT for citizens – both run by the Federal Ministry of the Interior (BMI) and its BSI agency; the Bundeswehr's CERT-BW with its war room and cyberdefence lab; federal state CERTs e.g. in the Ministry of Interior of Baden-Württemberg; and finally, private CERTs including Commerzbank, Telekom or Lufthansa.[89] Distinguishing between offence and defence is not always obvious, though, since testing one's own defences requires "penetration-testing" and the ability to intrude into systems.[90]

Adding offence to the equation

Other experts strongly disagree with the emphasis on defence, arguing that "in an offense-dominant environment, a fortress mentality will not work".[91] In the nuclear context, deterrence-by-denial approaches were largely inapt given the unbearable costs of defensive failure. In cyberspace, lack of clarity and credibility of punishment encourages cyberattackers to test defences and push their limits, defying deterrence-by-denial. The low cost, defined as the cost of conducting the attack plus the likely penalty, furthers the offensive advantage, as does the existence of a vast black market, offering anything from zero-day exploits, i.e. currently unknown software vulnerabilities, to off-the-shelf services to conduct denial-of-service attacks.[92] The nature of software development renders entirely avoiding bugs, or loopholes impossible, and quickly responding to attacks and closing vulnerabilities entails significant costs for the defender. Authors on cyberdeterrence-by-retaliation emphasise a number of key challenges and differences to classical deterrence.

When and whom to deter? Immediate vs. general deterrence and the challenge of attribution

Immediate vs. general deterrence is the question of whether deterrence is aimed at a specific adversary during an ongoing conflict or more generally at any would-be-offender during peacetime. Due to its development time and the need to know a system's vulnerabilities[93], cyberforce is little appropriate as a concrete deterrence measure once a conflict has erupted. On the other hand, retaliation against cyberattacks cannot be adhoc because of the need for time-consuming forensics. Thus, both general deterrence aiming to deter any attack by cyberforce as immediate deterrence by cyber means alone are improbable. Rather cyber can be an instrument in the broader toolbox.

[82] Cf. Bendiek 2012, 24-25

[83] Interview EDA Cybersecurity Official 2014

[84] Cf. Seidler 2011

[85] Cf. Reuters 2014

[86] Cf. Merkel 2014

[87] Bundeswehr brigadier-general Klaus Veit in Grunert 2013, 110

[88] Interview German BMVg Cyberdefence Official 2014

[89] Cf. CERT-Verbund 2014

[90] Interview NATO Cybersecurity Official 2014

[91] Lynn III 2010

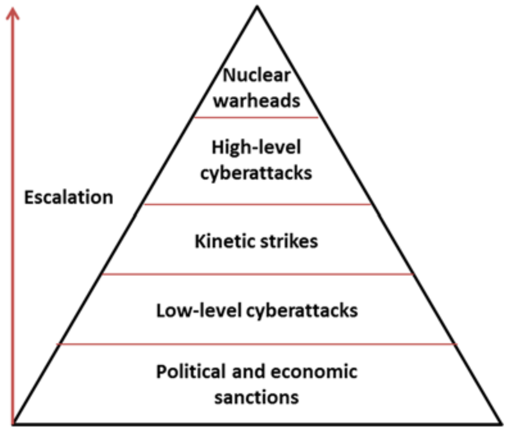
[92] Cf. Sheldon 2011, 97 and Interview EDA Cybersecurity Official 2014

[93] Cf. Cisco 2014, 37 describing the chain of steps required

Although suggested by some as an effective tool for immediate retaliation[94], active defence is ill-fitted for various technical, political and legal reasons. Such fully-automated retaliatory attacks may damage computers that are part of botnets without their owner's knowledge, while the botnet as a whole will simply replace the neutralised computer. Furthermore, nation states are not likely to legalise such mechanisms, thereby allowing private sector "corporate vigilantisms" to violate the government's monopoly on the use of force.[95] The multitude of actors entails further difficulties: During conflicts, patriotic and other hackers can engage in disruptive activities to add an unpredictable step of escalation. Governments may not be able to control these groups, weakening the implied promise of deterrence that "if you stop, we stop".[96]

Thus, "cyber threats are only meaningful when coupled with other, more traditional, threats."[97] In terms of retaliation in cyberspace, this may add additional levels of escalation: Firstly, escalation beyond political and economic sanctions using low-level cyberattacks and, secondly, escalating kinetic strikes ahead of threatening use of tactical nuclear warheads. [98] Figure 4 introduces a possible model. It can, however, be discussed whether kinetic strikes or high-level cyberattacks constitute larger escalation.

Figure 2: A possible model of escalation[99]



Since knowing the opponent is crucial in designing defensive or offensive responses, attribution is core. At the moment of an incident, it is difficult to assess whether one is dealing with a technical accident, indiscriminately spreading malware, or a targeted attack. Nevertheless, responses differ, whether dealing with state and state-sponsored actors or with cybercriminals. For deterrence-by-retaliation to work, aggressors must be convinced that they will be identified and punished; and attribution must be bulletproof to avoid creating new enemies and to convince third parties that the retaliatory measure is not an attack in itself.[100] Attribution was long thought impossible in cyberspace, and is still often called the key challenge to cyberdeterrence. The recent NATO CCDCOE study lists anonymity as "[denying] identification of malicious actors, thus making deterrence policies futile, the undertaking of diplomatic, political and economic reaction measures difficult, and the application of legal remedies, e.g. countermeasures, impossible".[101]

Still, "the attribution problem is partly artificial. As analyses of individual indictments following cyberattacks – both on the U.S. in 2013 and 2014 and Estonia in 2007 – demonstrate, attribution is costly and time-consuming, but possible. The major difficulty lies in prosecution once perpetrators are identified. In the Estonian case, Russia refused to prosecute indicted Russians, saying that their denial-of-service attacks did not amount to legal violations in Russia.[102] Tracking down perpetrators requires a number of tools since communications can be redirected via computers worldwide which hide the original perpetrator. In a conflict situation it is usually not difficult to determine the attacker's identity based on pure logic"[103]. Contextual attribution is based on knowing the conflict, the history and considering who benefits from the attack. It combines technical measures and intelligence operations to pinpoint the culprit. Dealing with state actors, malware source code and the programming style can be mapped against previous incidents. Such forensics revealed similarities between Stuxnet and Flame, intensifying accusations of U.S.-Israeli involvement in both high-complexity tools.[104] Both long-term rivals of Iran were singled out long before Snowden gave proof. State hackers have been observed to

[94] Cf. Kassab 2014, 60

[95] Interview EDA Cybersecurity Official 2014

[96] Libicki 2009, 62

[97] Sheldon 2012, 18

[98] Interview EDA Cybersecurity Official 2014

[99] Own figure on the basis of interview with EDA Cybersecurity Official 2014

[100] Cf. Libicki 2009, xvi, 72-73

[101] Ziolkowski 2013, XVI

[102] Interview NATO Cybersecurity Official 2014

[103] Interview EEAS Cybersecurity Official 2014

[104] Interview NATO Cybersecurity Official 2014 and EEAS Cybersecurity Official 2014

attack more consistently during their working day, and to only target what serves their strategic goals, which requires substantial knowledge about the system architecture. Private hackers are recognizable by their use of prevalent techniques and tools of the hacking community, rather than exploiting expensive zero-day vulnerabilities.[105]

Deterrence signalling against states is visible in cybersecurity strategies' insistence on international law. Political and technical experts concluded in the Tallinn Manual, drafted by a group of experts upon the invitation of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) that the law of armed conflict (LOAC) applies in cyberspace. Cybercriminals can be deterred with enhanced prosecution and reduced legal grey areas, while simply raising penalties will make the threat disproportionate and less credible. Cybersecurity strategies recognize this "need to emphasize the certainty of punishment over the severity of punishment", e.g. by supporting the Budapest Cybercrime Convention for globally harmonised legislation.[106]

What to deter? Narrow vs. broad deterrence

Considering narrow vs. broad deterrence the core question is "what is to be deterred?". In the current context, and based on initial definitions of operational and strategic cyberwar, a war of cyberattacks is highly unlikely. "Narrow" deterrence-by-retaliation requires unmistakable positioning as to what is acceptable and what is not. The outcomes of U.S. political cyberespionage and simultaneous indictment of Chinese officers for economic cyberespionage may set an important precedent. The U.S. draws somewhat artificial lines between political and economic cyberespionage, indicting Chinese officers for industrial espionage while itself spying on OPEC[107], hacking into China's Huawei Technologies and supporting, or at least tolerating, British hacking into Belgium telecommunications giant Belgacom.[108] The use of cyberattacks such as Stuxnet – which at an estimated cost of $100 million is relatively cheap compared to military hardware[109] – is dangerous, given the lack of international agreement on what is acceptable, and risks escalation. U.S. President Obama issued an executive order on 1 April 2015 calling for sanctions against individual and organised cyberattackers, especially those conducting attacks on critical infrastructure.[110] His cybersecurity adviser stated: "we want to have this tool available as a deterrent".[111] This is an important starting point.

The aforementioned Tallinn Manual insisted on the applicability of Geneva Convention IV on the protection of civilians in cyberspace. This prohibits disproportional attacks against civilian and non-military installations which must include critical civilian services such as banking. However, some discard specific "Cyber Geneva Conventions" as unverifiable and unlikely to yield results in the short- to medium-term, insisting instead on internationally agreed principles.[112] The UN's ITU sees hope in "effective norms against cyberaggression […] reining in unacceptable forms of behaviour".[113] Others, including the U.S. and Germany's Commissioner for International Cyberpolicy, oppose such a code of conduct at the UN level fearing interference with the openness of the internet.[114] However, international norms on restraint in cyberwarfare, rhetorically encouraged by U.S. Defence Secretary Hagel[115], appear the only hope to resolving diplomatic upsets about cyberespionage and cyberattacks.[116] The currently prevailing grey zones ultimately only serve the non-established powers and criminal actors. As a first step, nations worldwide must determine what constitutes illegal attacks and warrants responses from the international community. The protection of civilian critical infrastructure should be among the leading goals of such initiatives. Being mostly private-owned, the military and civilian government lack access and thus the means to ensure their security. The UN General Assembly and its working groups on cyber are currently the most appropriate forum to discuss which targets and which weapons are to be prohibited.

Military and political strategists can thereafter develop a narrow deterrence regime against specific actors, to protect certain systems and to single out weapons to be deterred. Cyberpower cannot be lever-

[105] Cf. Libicki 2009, 45, 47-48
[106] Freedman 2004, 65-66
[107] Cf. Spiegel, OPEC 2013
[108] Cf. Ferranti 2014 and cf. Spiegel, Belgacom 2013
[109] Cf. Gilbert 2014
[110] The White House 2015
[111] Eichensehr 2015
[112] Interview EEAS Cybersecurity Official 2014
[113] Harknett, Callaghan and Kauffman 2010 and cf. BMI IT Director Schallbruch in Grunert 2013, 111
[114] Cf. Spielkamp and Otto 2014, 12 and cf. Bendiek 2012, 25
[115] Cf. DefenceNews 2014
[116] Cf. Stevens 2012, 165, who discusses the need for credible force to back these norms

aged to deter any aggression against oneself, but outlining retaliatory steps in case of cyberattacks against a narrow set of targets or using a narrow set of attack mechanisms can render deterrence effective.

For whom? Central vs. extended deterrence

The question of central vs. extended deterrence extends beyond whether EU and NATO allies possess collective defence mechanisms, in their respective Article 222 of the Treaty on the Functioning of the European Union (TFEU)[117] and Article 5 of the North Atlantic Treaty.[118] For such deterrence to be effective, allies would have to signal to would-be-offenders that violations against one ally will result in a joint response. While the articles require considerable thresholds – the loss of human life arguably being one – the increasing connectedness of e.g. energy grids increases the threat for neighbours during cyberattacks against one country. NATO doctrine recognizes "cyber as part of NATO's collective defence"[119] and retaliation may be "by any means necessary".[120] NATO's lack of own offensive cyber-capabilities poses no problem therein since – similar to nuclear deterrence – member states could provide them while NATO provides its planning and coordination capabilities.[121]

Similar to any public-private cooperation, however, the contentious item is granting access to one's networks. Involving third countries – even if only to give proof of the perpetrator – requires revealing the damage dealt and thereby the vulnerabilities of one's system. [122] Public-private and civilian-military cooperation as well as inter-state collective cyberdefence requires a great deal of trust, since technical assistance can only be given if granted wide-ranging access, possibly revealing additional vulnerabilities.[123] Governments may, furthermore, consider it little desirable to take over operational tasks, e.g. in securing privately-owned critical infrastructure, as this may lead to free-riding and insufficient investment in their own cybersecurity. Given this unwillingness to grant access, NATO-coordinated joint cyberattacks seem unlikely.

As free-riding does not work in cyberspace, all nations have to, first and foremost, secure themselves. Secondly, the U.S. and other technologically leading NATO allies should engage in more strategic dialogue with its partners to ensure their preparedness. This can then be the basis for extended deterrence. President Obama strengthened the idea of such a concept, stating that "the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. ... We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, **our allies, our partners**, and our interests."*[124]*

[117] Cf. Official Journal of the EU 2012, 148

[118] Cf. European Commission, Cybersecurity Strategy 2013, 19: The EU's Strategy states that a "particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke [the Clause]".

[119] NATO 2014

[120] Interview NATO Cybersecurity Official 2014

[121] Interview EDA Cybersecurity Official 2014

[122] Cf. Libicki 2009, 50

[123] Cf. Libicki 2009, vxiii and Interview NATO Cybersecurity Official 2014

[124] The White House 2011, 14

Conclusion and outlook

Previous academic research on deterrence theory and its application to cyberspace, leads to a series of conclusions for policy-making. Deterrence theorist and former UK foreign policy advisor Sir Lawrence Freedman differentiates 1) deterrence-by-retaliation and deterrence-by-denial; 2) immediate vs. general; 3) narrow vs. broad; and 4) central vs. extended deterrence.

Taking into consideration the extensive literature review, it might be useful for German and European cyberdeterrence strategies to be inclusive of both retaliatory and denying mechanisms. This chiefly includes four elements: Firstly, resistance by developing strong guidelines against voluntary and accidental disruptions; secondly, resilience to quickly and fully recover from attacks; thirdly, the definition of clear-cut global rules on acceptable practice and legality of targets in cyberspace; and finally, a national strategy of responses within these rules, ranging from criminal prosecution and political condemnation to (economic) sanctions and, finally, measures of active defence and retaliation. Any retaliatory strategy must also address the question of whether kinetic strikes are warranted in the case of sincere damage to the property and lives of citizens.

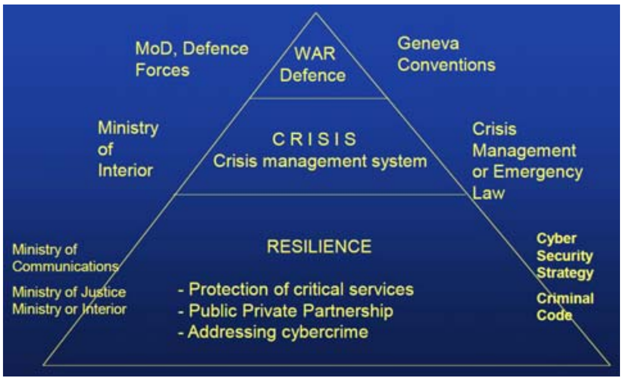
As "cyberweapons" require target-specific development, quick retaliatory cyberstrikes are impossible. Therefore, and due to the fact that attribution requires time-consuming forensics, retaliation with cyber means cannot be done ad-hoc. Defence and offence must thus be joined into a broader deterrence strategy. Those responsible for national defence, including Germany's BMVg in coordination with the BMI and the Foreign Office (AA), should focus on protecting their own networks, most importantly communication and weapons control. This will add credibility to any future deterrence strategy. However, deterrence strategies should start not merely from the defence community, but hand-in-hand with activities of the broader German government.

Currently, rather than strategically thinking about how to tackle threats, authorities are still trying to understand threat agents and vulnerability landscapes. Classical deterrence requires defining interests and drawing redlines. Threat assessment must identify the adversaries and develop appropriate responses for each of them. Germany must clarify its interests and priorities to be protected before deterrence postures – as a comprehensive combination of resistance, resilience and retaliation – can be effective. Which services and infrastructures are critical for the country's functioning? Which actors must cooperate to ensure their security? Purely focusing on the military is inappropriate, and while the military is good at defending its own networks, it has hardly any experience in cooperating with the public and, even less, the private sector. This, however, is an essential part of cybersecurity. To co-opt the private sector, governments have to create win-win-situations rather than imposing from above, and recognize that, unlike nuclear deterrence, cyberdeterrence is not a game of great powers and not even that of nation-states alone. Neither the European approach of imposed cooperation, as in the draft NIS Directive's mandatory reporting, nor the U.S. approach of largely leaving cybersecurity to market forces appear sufficient. Military responses are insufficient, requiring more than ever a comprehensive combination of tough rules and incentives, of carrots and sticks.[125]

While cyberdeterrence is reportedly not central in the German discourse[126], elements thereof are helpful in developing national responses. Policy-making may need to reconsider the differentiation of, on the one hand, Computer Network Operations (CNO) including Computer Network Attack (CNA) and Computer Network Exploitation (CNE) and, on the other hand, Computer Network Defence, including primarily IT-security. Considering all elements from the angle of deterrence theory may render overall cybersecurity and –defence more effective. Private actors can then be integrated, as evidenced in Germany's National Cybersecurity Council (NCSR) and National Cyberdefence Centre (NCAZ).[127]

[125] Cf. Lebow 2001, 128
[126] Interview BMVg Cybersecurity Expert 2014
[127] Cf. Unger 2013

Figure 3: EEAS figure on a possible inter-ministry division of labour[128]



Only the establishment of clear rules on acceptable practice in cyberspace, will enable broad and effective responses to prevailing threats. Nations and foreign nationals offending such treaties would then feel the deterring threat of retaliation with sanctions and criminals could be targeted with legal prosecution across national borders. Furthermore, the much emphasized role of the private sector would be strengthened, providing guidelines on how their defence mechanisms may themselves engage an attacker. The current grey zones in cyber conduct serve no one in the medium term. International agreements, similar to the Budapest Convention on Cybercrime, are crucial to preserving the internet as an engine of the global economy. The introduction of norms-based deterrence may thus provide a useful framework. Since cross-border cooperation is crucial, nation-states have to agree on acceptable thresholds, e.g. regarding the legality of cyberespionage. Similar to the beginnings of nuclear deterrence theory, when President Kennedy had to decide whether the Soviet placement of missiles in Cuba warranted a naval blockade, there is a lack of clarity on whether cyberattacks allow for kinetic retaliation. Norms-setting and confidence-building, rather than the deployment of offensive capabilities, may be the favourable course of action, to jointly tackle rogue attacks and cybercrime and to avoid escalation. There is a sense of urgency in statements of high-ranking military and political leaders, acknowledging the risks of making cars, hospitals, energy grids and even prisons controllable via the Internet. Reluctance to tackle these questions politically will complicate matters, as the private sector engages in politics and vigilantism by striking back against botnets[129] or – as in Google's case – threatening to end censorship of its queries in China.[130]

In order to achieve agreement on norms, it is sensible to build upon existing regimes such as the Geneva Conventions, establishing that similar offences through cyberspace warrant similar consequences as their traditional counterparts. The NATO CCDCOE "Tallinn Manual" and the "Peacetime Regime for State Activities in Cyberspace" are important and should be seen as the basis for any future efforts. In a first step of confidence-building measures, definitions on civilian critical infrastructures should be agreed upon internationally and undertaking or supporting attacks against all CI must be prohibited. This would move the discussion of whether or not cyberattacks are legitimate to the more relevant debate on which targets are acceptable, providing clarity for the development of effective military strategy. To accelerate much-needed progress, disagreements over the appropriate management of the internet as a whole (Internet Governance) or the provision of freedoms online should be dealt with separately from these debates.

[128] Own figure based on Tiirma-Klaar 2012, 5

[129] Cf. ZDNet 2011

[130] Cf. Markoff, Sanger and Shanker 2010

Annex

Glossary

Botnet[131]

A number of computers controlled by a single source and running software programmes and scripts. Can refer to distributed computing, e.g. for scientific purposes, but typically used in the mass infection of computers with malicious software for use in illegal activities without their owner's knowledge.

Critical infrastructures (CI)[132]

Physical resources, facilities, institutions, networks or services which, if destroyed or disrupted, would seriously impact the safety, security, health, or economic well-being of societies or the functioning of governments. These include: energy, information technology and telecommunication, transport, health, water and food, the finance and insurance sector, state and administration, media and culture. This may include SCADA systems (Supervisory Control&Data Acquisition), controlling (industrial) physical processes.

Distributed Denial-of-Service (DDoS) attacks[133]

Aimed at temporarily or permanently making machines or network resources unavailable to interrupt or suspend Internet services. Once a target server is saturated with external requests, it can no longer respond to legitimate traffic, or cannot do so within an acceptable period, typically forcing a system reset.

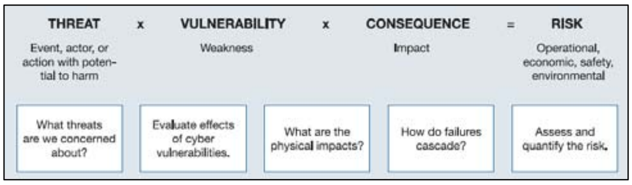
Man-in-the-middle attack[134]

In this method of active eavesdropping a third party introduces a listening mechanism between two parties, which believe that they are communicating directly with each other (e.g. a customer and the online-banking website). While both partners encrypt their data, the man-in-the-middle is able to read any communication, including passwords.

Risk management

The conscious process of understanding risks, of developing and of implementing actions to reduce risk to an acceptable level, given the implied costs. The risk level results from two factors: (1) the value of an asset to its owner/operator in case of loss or disruption, and (2) the likelihood of the risk to materialise.

Figure 4: Risk assessment[135]


THREAT
x
VULNERABILITY
x
CONSEQUENCE
=
RISK
Event, actor, or action with potential to harm
Weakness
Impact
Operational, economic, safety, environmental
What threats are we concerned about?
Evaluate effects of cyber vulnerabilities.
What are the physical impacts?
How do failures cascade?
Assess and quantify the risk.

Zero-day vulnerability or "0-day" *speak: [oh-day]*

A previously unknown software vulnerability, which offers a backdoor to bypass security mechanisms. Companies hire hackers to identify these loopholes in their own software, but the extensive black market often pays more. There are discussions to regulate sales of such exploits, e.g. prohibiting U.S. companies from selling them to blacklisted governments. Various such exploits were used in the 2010 U.S.-Israeli Stuxnet attack.[136] The "0" refers to the fact that it has been known for 0 days.

[131] Based on OSCE 2013, 90

[132] Based on BMI 2011, 15 and OSCE 2013, 90

[133] Based on OSCE 2013, 90

[134] Based on OSCE 2013, 90

[135] Based on OSCE 2013, 38 and 91

[136] On Stuxnet's zero-day exploits, see Bradbury 2012, 4

List of References

BBC. *US Pentagon to treat cyber-attacks as 'acts of war'.* 1 June 2011.

Bendiek, Annegret. “European Cyber Security Policy.” *SWP - Stiftung Wissenschaft und Politik/German Institute for International and Security Affairs.* October 2012.

—. “Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection.” *SWP - German Institute for International and Security Affairs.* March 2014.

Bentham, Jeremy. *The Works of Jeremy Bentham, 11 volumes.* Edited by John Bowring. Vols. Edinburgh: William Tait, 1838-1843.

Blitz, James. “UK becomes first state to admit to offensive cyber attack capability.” *Financial Times.* 29 September 2013.

BMI, German Federal Ministry of the Interior. *Cyber Security Strategy for Germany.* February 2011.

BMVg, German Federal Ministry of Defence. *White Paper 2006 on German Security Policy and the Future of the Bundeswehr.* 2006.

–. *Defence Policy Guidelines: Safeguarding National Interests – Assuming International Responsibility – Shaping Security Together.* 27 May 2011.

BMVg Cybersecurity Expert, interview by Tobias Metzger. (24 June 2014).

Bologna, Sandro, Alessandro Fasani, and Maurizio Martellini. “From Fortress to Resilience.” In *Cyber Security: Deterrence and IT Protection for Critical Infrastructures*, edited by Maurizio Martellini, 53-56. Heidelberg: Springer, 2013.

Bowen, Wyn Q. “Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism.” *Contemporary Security Policy*, Vol. 25, No. 1 April 2004: 54-70.

Bradbury, Danny. “SCADA: A critical vulnerability.” Computer Fraud & Security, Vol. 4, 2012: 11-14.

Brodie, Bernard, ed. *The Absolute Weapon.* New York, NY: Harcourt Brace, 1946.

Bush, George W. “Graduation Speech at West Point.” *The White House.* 1 June 2002.

CERT-Verbund. “Wer wir sind.” *Alliance of German Security and Computer Emergency Response Teams.* 2014. www.cert-verbund.de.

Chapman, Glenn. “Two Years and 100 M Dollars Buys Winning Cyber Army.” *Agence France-Presse*, 2010: August 1st,.

Cheswick, W, S. Bellowin, and A. Rubin. *Firewalls and internet security: Repelling the wily hacker.* Boston: Pearson Education Inc., 2003.

Cilluffo, Frank J., Sharon L. Cardash, and George C. Salmoiraghi. “A Blueprint for Cyber Deterrence: Building Stability through Strength.” *Military and Strategic Affairs*, Vol. 4, No. 3, 2012: 3-23.

Cimbala, Dr Stephen J. “Nuclear Deterrence and Cyber: The Quest for Conquest.” *Air & Space Power Journal*, March-April 2014: 87-107.

Cisco. *Cisco 2014: Annual Security Report 2014.* 16 January 2014.

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Ecco, 2012.

Council of Europe . *Convention on Cybercrime - Treaty Doc. 108-11, ETS No. 185.* 23 November 2001.

Davì, Marco. “Cyber security: European strategies and prospects for global cooperation.” *Carnegie Endowment for International Peace.* 11 November 2010.

Davis, Paul K. “Deterrence, Influence, Cyber Attack, and Cyberwar.” *RAND National Security Research Division - Working Paper.* June 2014.

DefenceNews. *Hagel encourages 'restraint' in cyber warfare.* 28 March 2014.

Dulles, John Foster. “The Evolution of Foreign Policy, Department of State Bulletin, XXX.” In *US Nuclear Strategy: A Reader*, edited by Philip Bobbit, Lawrence Freedman and Greg Treverton. London: Macmillan, 1989.

EDA Cybersecurity Official, interview by Tobias Metzger. (24 June 2014).

EEAS Cybersecurity Official, interview by Tobias Metzger. (27 June 2014).

Eichensehr, Kristen. The Cyber Sanctions Executive Order: What Will It Do and Will It Work?. justsecurity.org, 2 April 2015.

ENISA. *National-level Risk Assessments: An Analysis Report.* November 2013.

European Commission. “Cybersecurity Strategy.” *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* 7 February 2013.

EWI. “Critical Terminology Foundations 2: Russia-U.S. Bilateral on Cybersecurity.” *EastWest Institute.* Edited by James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko. February 2014.

Ferranti, Marc. “NSA hacked into servers at Huawei headquarters, reports say.” *Computerworld.* 23 March 2014.

Fischer, Michael, Jörg Blank, and Christoph Dernbach. "Germany confirms existence of operational cyberwarfare unit." *Deutsche Presse-Agentur.* 5 June 2012.

Freedman, Lawrence. *Deterrence.* Cambridge: Polity Press, 2004.

Freedman, Lawrence, ed. *Strategic Coercion: Concepts and Cases.* London: Oxford University Press, 1998.

Gaycken, Sandro, and Maurizio Martellini. "Cyber as Deterrent." In *Deterrence and IT Protection for Critical Infrastructures*, edited by Maurizio Martinelli, 1-10. Heidelberg: Springer, 2013.

Geers, Kenneth. "The challenge of cyber attack deterrence." *Computer Law & Security Review*, 2010: 298-303.

George, Alexander L., and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice.* New York: Columbia University Press, 1974.

German BMVg Cyberdefence Official, interview by Tobias Metzger. (24 June 2014).

Gilbert, David. "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog." *International Business Times.* 6 February 2014.

Goldman, Emily O., John Surdu, and Michael Warner. "The Cyber Pearl Harbor Analogy: An Attacker's Perspective." In *Cyber Analogies*, edited by Emily O. Goldman and John Arquilla, 26-32. Monterey: Naval Postgraduate School, 2014.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, Fall 2010: 102-135.

Grossman, Lev. "Inside the Code War." *TIME*, 2014: Vol. 184, No. 3: 20-27.

Grunert, Florian. "Ein Bericht über die Handelsblatt-Konferenz "Cybersecurity 2012" in Berlin." *Zeitschrift für Außen- und Sicherheitspolitik*, Vol. 6 2013: 107-112.

Guitton, Clement. "Cyber insecurity as a national threat: overreaction from Germany, France and the UK?" *European Security*, 2013: 21-35.

Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. "Leaving Deterrence Behind: War-Fighting and National Cybersecurity." *Journal of Homeland Security & Emergency Management*, 2010.

Hathaway, Melissa. "In Digital Combat, U.S. Finds No Easy Deterrent." *The New York Times.* 25 January 2010.

Kassab, Hanna Samir. "In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare." In *Cyberspace and International Relations: Theory, Prospects and Challenges*, edited by Jan-Frederik Kremer and Benedikt Müller. Heidelberg: Springer, 2014.

Kaufmann, William. *The Evolution of Deterrence 1945-1958.* Unpublished RAND research, 1958.

Knopf, Jeffrey W. "The Fourth Wave in Deterrence Research." *Contemporary Security Policy*, Vol. 31, No. 1 April 2010: 1-33.

Lebow, Richard Ned. "Deterrence and Reassurance: Lessons from the Cold War." *Global Dialogue*, Vol. 3, No. 4 Autumn 2001: 119-132.

Levin, Avner, Paul Goodrick, and Daria Ilkina. "Securing Cyberspace: A Comparative Review of Strategies Worldwide." *Ryerson University - TED Rogers School of Management. Privacy and Cyber Crime Institute.* 2013.

Lewis, James A., and Katrina Timlin. "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization." *Center for Strategic and International Studies (CSIS) and United Nations Institute for Disarmament Research (UNIDIR).* 2011.

Libicki, Martin C. "Brandishing Cyberattack Capabilities." *RAND National Defense Research Institute.* 2013.

—. "Cyberdeterrence and Cyberwar - Prepared for the United States Air Force." *RAND Corporation.* 2009.

Lieber, Keir. "The Offense-Defense Balance and Cyber Warfare." In *Cyber Analogies*, edited by Emily O. Goldman and John Arquilla, 96-107. Monterey: Naval Postgraduate School and U.S. Cyber Command, 2014.

Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs Journal.* September/October 2010.

Malone, Patrick J. *Offense-Defense Balance in Cyberspace: A Proposed Model.* Monterey: Naval Postgraduate School, 2012.

Marchive, Valéry. "Cyberdefence to become cyber-attack as France gets ready to go on the offensive." *Vive la tech.* 3 May 2013.

Markoff, John, David E. Sanger, and Thom Shanker. "In Digital Combat, U.S. Finds No Easy Deterrent." *The New York Times.* 25 January 2010.

Markoff, Michele. "Remarks by Michele Markoff, Deputy Coordinator for Cyber Issues, Office of the Secretary of State, at the First Committee Thematic Discussion on Other Disarmament Issues and International Security, New York." *The United States Mission to the United Nations.* 30 October 2014.

Mason, Rowena. "Labour urges strategic defence review to consider cyberwar threat." *The Guardian.* 24 March 2014.

Maurer, Tim. *Cyber Norm Emergence at the United Nations. An Analysis of the UN's Activities Regarding Cyber-security.* Cambridge: Belfer Center for Science and International Affairs, 2011.

Merkel, Angela. *Podcast - Kanzlerin Merkel: "Neue Projekte mit Frankreich" und Datenschutz.* 15 February 2014.

Morgan, Patrick. *Deterrence Now.* Cambridge: Cambridge University Press, 2003.

—. *Deterrence: A Conceptual Analysis.* Beverly Hills, CA: Sage Publications, 1977.

NATO CCDCOE. *Peacetime Regime - Newsletter.* n.d. http://www.ccdcoe.org/peacetime-regime.html.

NATO Cybersecurity Official, interview by Tobias Metzger. (30 April 2013).

NATO Cybersecurity Official, interview by Tobias Metzger. (17 June 2014).

NATO. *NATO steps up collective defence, support for reforms in Ukraine.* 3 June 2014.

Nye, Joseph S. *The Future of Power.* New York: PublicAffairs, 2011.

Official Journal of the EU. "Consolidated Version of the Treaty on the Functioning of the European Union." 26 October 2012.

OSCE. *Good Practices on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Guide Focusing on Threats Emanating from Cyberspace.* 2013.

Oxford English Dictionary. *Oxford English Dictionary online - "deter".* 2014.

Oxford Reference. *Oxford Dictionary for Scientific Writers and Editors online.* n.d.

Philbin, Lt. Col. Michael J. "Cyber Deterrence: An Old Concept in a New Domain." *U.S. Army War College: Strategy Research Project.* March 2013.

Powell, Robert. *Nuclear Deterrence Theory: The Search for Credibility.* Cambridge: Cambridge University Press, 2008.

Quester, George. *Offense and defense in the international system.* New York: Wiley, 1977.

Reuters. *China bans use of Microsoft's Windows 8 on government computers.* 20 May 2014.

Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World.* Washington D.C.: Georgetown University Press, 2012.

Rid, Thomas. "Think again: Cyberwar. Foreign Policy. Retrieved September 20, 2012 from." *Foreign Policy.* 27 February 2012.

Schelling, Thomas. *Arms and Influence.* New Haven: Yale University Press, 1966.

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York: Cambridge University Press, 2013.

Schwarz, Klaus-Dieter (2005). Die Zukunft der Abschreckung. SWP-Studien 2005/s13, June 2005.

SDA. "Annual conference." *Conference Report: Overhauling transatlantic security thinking.* 15 July 2014.

—. "Evening debate - At a glance." *Critical infrastructure protection in the cyber-age: Evening debate - At a glance.* 30 June 2014.

—. *Evening debate: Critical infrastructure protection in the cyber-age.* Brussels. 30 June 2014.

Secretary of Defence Panetta, Leon E. *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City.* 11 October 2012.

Seidler, Felix. "Sicherheit im Cyber-Space: Nicht sicher, nur sicherer ." *Seidlers Sicherheitspolitik.* 31 July 2011.

Shaheen, Salma. "Offense-Defense Balance in Cyber Warfare." In *Cyberspace and International Relations: Theory, Prospects and Challenges*, edited by Jan-Frederik Kremer and Benedikt Müller, 77-94. Heidelberg: Springer, 2014.

Sheldon, John B. "State of Art: Attackers and Targets in Cyberspace." *Journal of Military and Strategic Studies*, Vol. 14, Issue 2, 2012: 1-19.

—. "Deciphering Cyberpower: Strategic Purpose in Peace and War." *Strategic Studies Quarterly*, Summer 2011: 95-112.

Simpson, Emile. *War From the Ground Up: Twenty-First-Century Combat as Politics.* Oxford: Oxford University Press, 2013.

Snyder, Glenn. *Deterrence and Defense.* Princeton: Princeton University Press, 1961.

—. *Deterrence by Denial and Punishment.* Princeton: Center of International Studies, 1958.

Spiegel. "Belgacom." *Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm.* 20 September 2013.

—. "OPEC." *Oil Espionage: How the NSA and GCHQ Spied on OPEC.* 11 November 2013.

Spielkamp, Matthias, and Philipp Otto. "Interview mit Dirk Brengelmann: Die Fragmentierung des Netzes ist eine der großen Gefahren." *Der Digital Wandel: Magazin für Internet und Gesellschaft*, Q1 2014: 10-13.

State Department. *International Cyber Diplomacy: Promoting Openness, Security and Prosperity in a Networked World.* 14 July 2011.

Stevens, Tim. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy*, Vol. 33, No. 1 April 2012: 148-170.

The White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* May 2011.

The White House. “Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.” Contemporary Security Policy, 2013: 254-256.

The White House. Executive Order. "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". 01 April 2015.

Tiirma-Klaar, Heli. “Presentation: National Cyber Security Strategies and International Cyber Policy.” *European External Action Service.* 22 October 2012.

Unger, Christoph. “E-lecture: Schutz kritischer Infrastrukturen als Element der Cybersicherheit.” *Unversität Hamburg.* 20 November 2013.

van Evera, Stephen. “Offense, defense and the causes of war.” *International Security*, 1998: 5-43.

ZDNet. *Microsoft kills MacDefender scareware botnet.* 29 September 2011.

Ziolkowski, Katharina, ed. *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy.* Tallinn: NATO CCDCOE, 2013.