Alex Tanchev

AUSTRIA INSTITUT FÜR EUROPA- UND SICHERHEITSPOLITIK

FOKUS | 7/2018

The strategic dimensions of cyber-security – an interdisciplinary approach

With the 2016 US Presidential Election, the question of cyber-security entered the mainstream and set the focus on how nations and other entities use cyber-space as an extension of their "real-world" agendas. This question is by no means new, yet it has remained somewhat overlooked, perhaps, not in small part due to the dynamism, complexity and technicality of the subject, acting as gatekeepers for novices. That being said, a certain level of understanding about cyber-security could be reached through combining approaches from other fields, international relations, political science, security studies to name a few, in order to see the "big picture" and how the geostrategic ambitions of actors could be reflected in cyber-space. Furthermore, in the near future, technology will continue to become a more and more integral part of our everyday lives, so awareness of the possible threats and mindfulness of our actions are key to mitigating the possible dangers that our societies might face.

This brief overview will attempt to provide the necessary basis upon which further knowledge could be built, looking at the rules and actors of cyber-space. These segments, along with how future developments would affect the sector cannot be done justice in such a limited format, so this text should be viewed as a roadmap to where the main debates in the field lie.

To begin with, an oft-cited characteristic of cyber-space is the vagueness and ambiguity of the language used to describe the occurrences in the virtual world. At the time of writing, there is no universal consensus of what exactly constitutes a cyber-attack, let alone cyber-war. Cyber-espionage and cyber-crime, for example, fall into the graph of what is considered a cyber-attack, however, they are seen as "routine occurrences",[1] separate from acts of war. An example of this, are the attacks on Estonia in 2007 which were perceived as individual cyber-crimes and not operations that call for the use of Article 5 of the NATO Treaty.[2] In that sense, the three characteristics that must be present for an act of war, to be considered as such, are its violent nature, instrumentality and political purpose.[3] The Tallinn and Tallinn 2.0 manuals look deeper into this debate and try to set the legal framework for future legislation and try to set the stage for where the red line should be in an international convention.

Furthermore, a distinction must be made by "technical computer security" – which is at the center of computer science studies and "cybersecurity" – an aspect of national security.[4] Nissenbaum argues that the former focuses on protecting individuals, while the latter puts the emphasis on protecting the state entity from foreign threats.[5] This might seem like a mere question of semantics, however, ultimately it is important when deciding who should govern cyber-space and what the rules are. The virtual world is a domain where the logic of national borders does not apply – it is not a conquerable and controllable realm.[6] At the same time, critical infrastructure is often vulnerable and targeted by malicious attacks, so states attempt to do all in their power to protect it. This overlap between the public and the private sector further complicates the debate of how the cyber-world should be managed and brings forth the questions of civil liberties, free flow of information and the equal treatment of all data.

While the debates for the access to personal information and net neutrality lie beyond the scope of this paper, the next section will focus on the rules that are "naturally" characteristic of the cyber-sphere due to technological and behavioral specifics, how they are exploited and what strategies could be employed to govern it.

Rules, Threats and Doctrines

Cyber has officially been recognized as a fifth domain of warfare, along with air, land, sea and space.[7] As such, states see the possibility of it remaining ungoverned as a potential weak link which could threaten their national sovereignty.[8] In that sense, strategists have tried to transfer the lessons learned from the real world to the virtual one and apply doctrines such as deterrence and mutually assured destruction to it, without acknowledging the fact that the norms of cyber-space differ quite radically from what they are used to deal with.

As a start, the standard logical triptych of **attribution - retaliation - deterrence** became, at most, ineffective. While kinetic attacks and real-world acts of aggression can always be traced back to an individual, organization or states, in cybers-pace that becomes problematic. Attackers could hide their origins by technical means, namely rerouting their signal to different parts of the world before committing the attack. Cyber-security forensic teams can, in some cases, track the origin of the attack, however, that is traditionally very time and resource-consuming – around 200 days, with costs in the millions.[9] It must be noted that these numbers can increase dramatically, depending on the caliber of the attack.[10]

After the origin has been identified, a second problem arises – attributing the operation to an accountable target. Even if the perpetrator is discovered, there is often no concrete way, in which his actions can be tied to the desires of a country's military or government, rather than his own free will.

That, then, makes deterrence inapplicable. Tomas Schelling argues that the best way for deterrence to work is to signal your commitment for retaliation in a way that

will hurt the attacker – if that commitment is credible and the attacker has more to lose than to gain, deterrence would be a success.[11] If credible punishment is negated due to the lack of attribution beyond a reasonable doubt, malicious activities will continue without any fear of repercussions.

Another factor that contributes to the ineffectiveness of the attribution – retaliation – deterrence chain is the fact that **geographic proximity** to the place of the attack **does not play a role**. Malicious activities could be carried out half the world over with the same effectiveness as if the person were in the same city. Moreover, if the attacker is located in a different country, then the local authorities would be the ones who have jurisdiction to punish the culprit. Lastly, coordinated attacks are not limited by the physical distance and can be carried out by immense speed, making it difficult to determine "who shot first".[12]

The ease with which attacks can be carried out with little consequence has let actors cause a lot of damage with relatively little investment.[13] This **asymmetry** is further exacerbated by the fact that the attacker typically has the upper hand.[14] Cyber-defenses are static and even a small gap can be exploited and used to compromise the whole system. At this point in time, technology cannot be protected by an air-tight method and actors, accepting this, can decide to invest heavily into offensive capabilities. Former U.S. Deputy Secretary of Defense William Lynn even argues that "cyber-warfare is like maneuver warfare, in that speed and agility matter most".[15] This **cult of the offensive mentality** has further led to a spiral of mistrust[16] between actors that, if taken to the extreme, can lead to a race to the bottom where every system in the world is infiltrated and is one click away from disaster.

The cyber-world is also **all-encompassing in nature** – it is not limited to the public or private spheres. The market's invisible hand is the one that sets trends and drives progress, while actors adopt a reactive stance. In that sense, military and government structures are grossly outpaced by the **dynamism** in the sector. As an example, we can look at the Pentagon, which requires 7-8 years to implement a computer system after it was first introduced on the market – by that time, by Moore's law, it is already several generations behind state-of-the-art technology.[17]

We can see a similar development in the legal frameworks of states – it took almost half of the countries that signed the Budapest Convention on Cyber Crime a decade or more to ratify the agreement due to the time required to actually develop appropriate laws.[18] In that sense, law-makers are faced with a paradox – they can either focus on the technological aspect of the cyber-world, which might get outdated by the time their legislation comes into force; or they can try and regulate human behavior, which is likely to clash with the very idea of the Internet as an open space where absolute freedom of expression is the norm.

Despite the vast number of different types of cyber-attacks,[19] they can roughly be grouped into three clusters[20] – ones that aim to gather information (espionage), ones that focus on causing damage (sabotage) and ones that use more subtle tools to attack the accepted social order (subversion).

The Tallinn Manual defines **cyber-espionage** as "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather information with the intention of communicating it to the opposing party".[21] Here, it must be noted, that all states engage in spying in one form or another[22] – countries would look to technically advanced adversaries, while the latter use the same technological edge to stay informed on what the other actors in the world are doing. There are countless examples of operations of that sort – from Gauss, which stole passwords and data[23] to Flame, which took screenshots and recorded audio,[24] but perhaps the most famous ones are Moonlight Maze and GhostNet. The Moonlight Maze virus infiltrated the US Department of Defense, Department of Energy and NASA and leaked thousands of pages of sensitive information.[25] GhostNet, on the other hand, was used to monitor critical political, media and economic locations in 103 countries.[26]

The most interesting thing about these two cases, however, is not who the perpetrators were or the type of information that got stolen. The fascinating part is that they remained undetected for prolonged periods of time. Further, it is impossible to distinguish if an attack is "benign" in nature and only aims at gathering information, or whether there is a switch that would damage the system the infiltration is in – the difference is only visible when the effects are felt.[27] Arguably, if you can spy on a network, you can manipulate it.[28]

The infamous Stuxnet virus is a prime example of how fine the line between espionage and **sabotage** is. It infiltrated very specific hardware in Iranian nuclear facilities, where it remained dormant and monitored the processes in the facility. After a pre-determined trigger was activated, however, it took over control and began feeding the security systems false information.[29] The result was substantial damage and a delay in Iran's nuclear programme.[30]

This incident shows the potential of what highly sophisticated intrusions are capable of. There are 16 sectors that are considered in the sphere of critical infrastructure – 90% of them owned by private companies, yet highly sensitive for national security and all of them potentially vulnerable to cyber-attacks.[31] Furthermore, Stuxnet is not an isolated case. We see malicious attacks evolving in complexity and build on the lessons learned from the attack on Iran, as in the case of TRITON which targeted industrial control systems with the intent of causing physical damage.[32]

These examples of major breaches present several important lessons. First, a lot of the information on them is classified – attackers and sometimes targets can remain unnamed with the goal of covering the gaps in security, the tools that were utilized and the reputation of the victim. Second, is the caliber of the viruses – they could have as much as 20 times more code than average malware, contain no bugs and leave no trace while also spreading

without the need for human interaction.[33] Lastly, these attacks are not something that can be built by a small group of enthusiasts in a short period of time – they require an enormous amount of dedication, both resource and timewise. This has led analysts to believe that only nation-states are capable of such operations.[34]

With the inherent inability of victims to protect themselves from all attackers and the low probability of being held responsible for the attack, cyber-operations might seem like the ultimate weapon. However, a closer examination tells a different story. In reality, the Stuxnet attack did delay the Iranian nuclear programme by about a year but it was far from putting an end to it. The period was then followed by a huge spike in the number of centrifuges that Iran had installed, and the scale of the nuclear facilities grew exponentially.[35] In addition, it put the code of the malware in the hand of the Iranians as well as other infected states,[36] which then reverse-engineered it and used it for their own benefit.[37] It must also be noted that the attack on the Islamic Republic led a number of talented youths to join the Iranian Cyber Army and increase the country's cyber-capacity. Lastly, the gap between nation-states and non-state actors in their ability to target industrial control systems is closing due to underground marketplaces where malicious code is sold. While it is still not a cause for alarm, it must be considered when analyzing future developments in the sector.[38]

Due to the high costs and questionable benefits, some actors might decide to choose more subtle ways to use the technological capabilities of the new era. Through methods of **subversion** and propaganda less technologically developed nations or countries that lack the resources for a comprehensive cyber-programme can deepen societal cleavages, enforce prejudices and promote tribalism, while also spreading disinformation. FireEye warns[39] of the role unauthentic media plays in information operations – social media has already acted as an amplifier for social grievances and despite proof of involvement of foreign actors in the 2016 US elections and certain debates in the EU, little has been done to counter these operations. These methods are employed by actors that see cyber-security as a marathon and not a sprint, relying on the erosion of societal trust; focusing on the silent, rather than the visible. These problems will only continue to grow in importance with the upcoming elections in the Europe, the Middle East and Africa in 2019. Malicious information campaigns are expected to become even more difficult to detect, while the cases of tactical leaking of sensitive information are likely to grow in number.[40]

As the threat landscape evolves, however, actors, and in particular - countries, have developed different doctrines to consolidate their efforts to minimize the damages, caused by malicious intent. That way governing bodies can better decide where to allocate resources while also signaling their intentions and priorities[41]. Mulligan and Schneider argue that means and goals have to be identified before we can talk about a comprehensive cyber-security policy.[42]

Perhaps the most intuitive is the **doctrine of prevention,**[43] although, as already discussed, absolute security at this moment seems improbable due to the upper hand that offense has over defense. Even if a perfect Great Firewall were to be erected to protect software, there will always be the human element in any system. An estimate of about 90% of attacks occur through social engineering practices or users not updating their operating systems with the latest patches.[44]

When actors accept their system will inevitably be infiltrated, they might turn to the **doctrine of risk management.**[45] The goal here is to reduce the benefits the attackers gain or the losses that defenders suffer. This axiom allows decision-makers to try and protect only a limited scope of critical assets. The weak point in this doctrine is that information about attacks might not be publicly available, which, in turn, makes prevention difficult and limits the understanding of attacker motivations as well as the ability to make adequate risk calculations.[46] This approach might gain popularity if information sharing became more open and analysts can use datasets to actually put "price tags" on breaches.

Despite all the obstacles that have to be overcome, the doctrine of **deterrence through accountability** is one that nation-states often look to.[47] It has also garnered some successes with arrests, linked to the Fin7 hacking group[48] as well as agents from Russian Military Intelligence Directorate (GRU)[49] However, this doctrine goes against the very things that make the Internet an environment based on the free flow of information, freedom of speech and anonymity. Further, it also gives the defender a very passive role that relies on punitive actions, instead of proactively encouraging them to protect their assets.

Mulligan and Schneider propose an alternative doctrine – **cyber-security as a public good.**[50] Since it is non-rivalrous and non-excludable cyber-security resembles other public goods like healthcare. Its ideal goals would be to balance individual rights with public well-being. At this moment the lack of consensus on terms like what constitutes "insecurity" and "cyber-security" lead to different doctrines of cyber-security[51] but the focus lies on prevention, mitigation, containment and recovery strategies.

Perhaps the most important lessons stakeholders can learn from these doctrines are the importance of the capacity to respond to large-scale incidents, the protection of critical infrastructure, the collaboration with other entities when an attack occurs and, last but not least, the development of a cyber-hygiene and security culture.

These rules and axioms determine how actors behave in cyber-space, so it is essential to understand who the stakeholders are and how they interact with each other.

Actors and cooperation

Nation-states are still the prime example of an actor online with their vast amount of resources and credibility in the field of international relations. With the rise of im-

portance of the cyber-domain, they have begun to re-assert their sovereignty in the virtual world.[52] There are four components that characterize a country as cyber-power in today's security landscape – they must have large and/or technologically advanced economies, the government's ability to work with the private sector, aggressive information and intelligence agencies and the ability to build a narrative that others can get behind.[53] State actors can roughly be grouped into three categories – Enablers, Disruptors and Survivors.

Enablers are the states that perpetuate the current system in cyber-space. The creator of the Internet – the US, naturally, falls into this group, as well as most other democracies that promote free information-sharing between all online users. Typically, enablers are technologically advanced and benefit from the current state of the system, however, analysts like Adam Segal expect the downfall of the digital Pax Americana due to their much more aggressive competitors.[54]

Disruptors, on the other hand, see the unregulated exchange of information as a threat to their national security and ruling regimes. Typically, these are emerging cyber-powers with strong centralized governments. China, for example, has built its own version of the Internet and is highly suspicious of foreign influence in their digital space.[55]

Lastly, survivors rely on the inherent asymmetry of cybers-pace, through which they could reap high rewards with relatively little investments, in order to increase their international renown and protect their physical borders. Typical examples are North Korea and Iran who feel threatened by their neighbors and, in the case of conflict, would rely on disrupting the control and command operations of their enemies' superior forces and over-reliance on technology.

While the focus falls on state actors the role and capabilities of **non-state actors** must not be overlooked. While the biggest victims of cyber-attacks are medium and large companies,[56] their role is mostly passive, and they rarely play a part in shaping the cyber landscape despite their, sometimes large, economic potential. Active non-state actors can be classified into several groups, each with distinct tactics, techniques and procedures.[57]

Cyber-criminals are mainly motivated by financial benefits. They mainly rely on attacking the human element of the security system through social engineering. Their attacks are low-cost and easy to pull off, however, they rely on the poor digital culture on at least some of their targets. In that case, their goal is to reach as many people as possible through spam campaigns.

Hacktivists, unlike cyber-criminals, are not motivated by money and rather target the source of their perceived grievances. The motives are difficult to predict in advance; nonetheless, they rely mostly on the so-called cyber-vandalism. They target websites (or social media accounts, if their victim is an individual) in order to tarnish their reputation. Hacktivists can be lone-wolves, or they can be groups of people like the notorious Anonymous.[58]

State-sponsored actors, on the other hand, are still relatively uncommon,[59] however, their role is likely to increase, if attribution were to become more effective. Their goals coincide with that of nation-states and can target sensitive information or critical infrastructure, relying on multiple angles of attack simultaneously. They are usually organized in coordinated groups that work together and have both more time and resources than any other non-state actor which makes defending against them difficult.

Interestingly, supranational organizations also try to react to the growing importance of the cyber realm. NATO[60], the EU[61] and the UN[62] act as instruments that try to consolidate and coordinate the efforts of their members in order to establish a set of widely accepted rules in the virtual world. Only through international cooperation can the most critical cyber-security risks be mitigated.[63] Currently, a lot of the information remains hidden from the public in the fear that it will ruin the victim's reputation or that the knowledge might fall into the wrong hands, which significantly hampers the clarity of what actors must deal with and how they should react. Former CIA and NSA director Michael Hayden even argues that the field of cyber-security is overclassified.[64] Historically, the situation has been similar with the questions of biological and nuclear warfare, arguing also that the complexity of the science and verification methods act as barriers for international agreements[65] but as time passed and these questions entered the public sphere more and more, it turned out that opposing factions managed to reach an understanding.

Right now, the proverbial Pandora's box has been opened. Actors do whatever they can get away with, riding a spiral of instability since deterrence through the threat of retaliation by attribution is still mostly ineffective. As a global community, there are three areas that we can rely on to improve our security posture – technology and innovation by enabling the free flow of information - research breakthroughs are what keeps us safer; investment in educating people – radical self-responsibility should be taught to people so that they know what to look out for; and diplomacy – all actors, regardless of their affiliations are in this threat environment together. Only through settling the rules of engagement can we avoid the risks of escalation.

Alex Tanchev is currently an intern at the Austrian Institute for European and Security Policy. He completed his Bachelor's degree in International Relations in the University of Sofia „St. Kliment Ohridski", Bulgaria and is currently enrolled in the Master of Political Science programme in the University of Gothenburg, Sweden. His previous experience includes working for the Bulgarian Academy of Sciences, Sofia Security Forum, the U.S. Embassy in Sofia and the online platform for international relations students E-IR.

Endnotes

1) James Andrew Lewis (2010), 'The Cyber War Has Not Begun', Center for Strategic and International Studies, p. 2.
2) Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security - Christian Czosseck, Rain Ottis and Anna-Maria Talihärm Cooperative Cyber Defence Centre of Excellence, Available at: https://ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_the_2007_Cyber_Attacks.PDF
3) Thomas Rid (2012), 'Cyber War Will Not Take Place', Journal of Strategic Studies, Vol. 35, pp. 5-32
4) Where computer security meets national security - Helen Nissenbaum Department of Culture and Communication, New York University, Available at: https://nissenbaum.tech.cornell.edu/papers/ETINsecurity.pdf
5) Ibid.
6) Myriam Dunn Cavelty (2012), 'The Militarisation of Cyber Space: Why Less May Be Better', 4th International Conference on Cyber Conflict, Tallinn, NATO CCD COE, p. 12.
7) 2018 National Defense Strategy of the USA, Available at: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
8) The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age – CFR, Available at: https://youtu.be/6jgiad44r7c
9) How long does it take to detect a cyber-attack? – Luke Irwin, IT Governance USA, Available at: https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack
10) Breach Detection by the Numbers: Days, Weeks or Years – Infocyte, Available at: https://infocyte.com/blog/2016/07/26/how-many-days-does-it-take-to-discover-a-breach-the-answer-may-shock-you/
11) Schelling, T. C. (1966), "2", The Diplomacy of Violence, New Haven: Yale University Press, pp. 1–34
12) Nicholas Tsagourias (2012), 'Cyber-attacks, self-defense and the problem of attribution', Journal of Conflict and Security Law, Vol. 17. p. 234.
13) 60 Must-Know Cybersecurity Statistics for 2018 – Rob Sobers, Varonis, Available at: https://www.varonis.com/blog/cybersecurity-statistics/
14) Cyberwarfare: Play Offense Or Defense? – Gadi Evron, Available at: https://www.darkreading.com/risk/cyberwarfare-play-offense-or-defense/d/d-id/1133181
15) Defending a new Domain – W.J. Lynn, Foreign Policy, Available at: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain
16) Cooperation Under the Security Dilemma, Robert Jervis, World Politics, Vol. 30, No. 2 (Jan., 1978), pp. 167-214 Available at: http://www.sscnet.ucla.edu/polisci/faculty/trachtenberg/guide/jervissecdil.pdf
17) Defending a new Domain – W.J. Lynn, Foreign Policy, Available at: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain
18) Cooperation Under the Security Dilemma – Robert Jervis, World Politics, Volume 30, Issue 2, Available at: http://www.sscnet.ucla.edu/polisci/faculty/trachtenberg/guide/jervissecdil.pdf
19) Top 10 Most Common Types of Cyber Attacks – Jeff Melnick, Available at: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
20) Cyber War Will Not Take Place Thomas Rid, Hurst Publishing ,2017
21) Tallinn Manual on the International Law Applicable to Cyber Warfare, CUP 2013,.Available at: http://csef.ru/media/articles/3990/3990.pdf
22) News Flash: States Spy on Each Other – Stephen Walt, Foreign Policy, 2013 Available at: https://foreignpolicy.com/2013/07/01/news-flash-states-spy-on-each-other/
23) oint Security Awareness Report (JSAR-12-222-01), Available at: https://ics-cert.us-cert.gov/jsar/JSAR-12-222-01
24) Joint Security Awareness Report (JSAR-12-151-01A), Available at: https://ics-cert.us-cert.gov/jsar/JSAR-12-151-01A
25) Major Schaap, Arie J. "Cyber Warfare Operations: Development and Use Under International Law." Cardozo Journal of International and Comparative Law, Vol 64, p. 121–172. 2009. Available at: http://www.afjag.af.mil/shared/media/document/AFD091026024.pdf ; The First Cyber Espionage Attacks: How Operation Moonlight Maze made history – Chris Doman, 2016, Available at: https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7
26) Chinese hackers 'using ghost network to control embassy computers' – Mike Harvey, The Times 2009, Available at: https://www.thetimes.co.uk/article/chinese-hackers-using-ghost-network-to-control-embassy-computers-hxh30tbn7kb
27) Media Room – Cybersecurity, An Introduction - Paul Rosenzweig, Available at: http://www.paulrosenzweigesq.com/media-room/media-room-cybersecurity-introduction/
28) Zero Days (2016) – Writer and Director - Alex Gibney
29) Siemens: Stuxnet worm hit industrial systems – Robert McMillan, 2010 Available at: https://www.computerworld.com/article/2515570/network-security/siemens--stuxnet-worm-hit-industrial-systems.html
30) Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? - David Albright, Paul Brannan, and Christina Walrond , Institute for Science and International Security, 2010 Available at: http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf
31) The 16 Sectors of Critical Infrastructure Cybersecurity, Available at: https://blog.cipher.com/the-16-sectors-of-critical-infrastructure-cybersecurity
32) Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure - Blake Johnson et.al. 2017, Available at: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
33) Zero Days (2016) – Writer and Director - Alex Gibney
34) Stuxnet was work of U.S. and Israeli experts, officials say - Ellen Nakashima and Joby Warrick, 2012, Available at: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.c5d60bd0f337
35) Zero Days (2016) – Writer and Director - Alex Gibney
36) Stuxnet Virus Infected Russian Nuclear Reactor, Expert Says, Oded Yaron, 2013, Available at: https://www.haaretz.com/.premium-stuxnet-infects-russian-reactor-1.5288976
37) THE NSA ACKNOWLEDGES WHAT WE ALL FEARED: IRAN LEARNS FROM US CYBERATTACKS - Kim Zetter,2015 Available at: https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/
38) Intelligence Declassified - Sandra Joyce, FireEye 2018, Available at: https://content.fireeye.com/predictions/rpt-security-predictions-2019
39) From the Files of FireEye Threat Intelligence - FireEye 2018, Available at: https://content.fireeye.com/predictions/rpt-security-predictions-2019
40) Ibid.
41) The US doesn't just need a cyber policy, it needs a cyber doctrine – Megan Reiss, 2017, Available at: https://www.washingtonexaminer.com/the-us-doesnt-just-need-a-cyber-policy-it-needs-a-cyber-doctrine
42) Doctrine for Cybersecurity - Deirdre K. Mulligan and Fred B. Schneider, 2011 Available at: https://www.cs.cornell.edu/fbs/publications/publicCybersecDaed.pdf
43) Ibid.
44) The Hacked World Order: Elements of Cyber Power - Adam Segal, Council on Foreign Relations, 2016, Available at: https://www.cfr.org/blog/hacked-world-order-elements-cyber-power
45) Doctrine for Cybersecurity - Deirdre K. Mulligan and Fred B. Schneider, 2011 Available at: https://www.cs.cornell.edu/fbs/publications/publicCybersecDaed.pdf
46) Rainer Boehme and Galina Schwartz. Modeling Cyber-Insurance: Towards A Unifying Framework. Working paper presented at Workshop on Economics of Information Security, Harvard University, June 2010. Available at: http://weis2010.econinfosec.org/papers/session5/weis2010 boehme.pdf
47) Butler W. Lampson. Computer security in the real world. IEEE Computer 37(6), June 2004, 37–46.
48) THE BILLION-DOLLAR HACKING GROUP BEHIND A STRING OF BIG BREACHES - Lily Hay Newman, 2018, Available at: https://www.wired.com/story/fin7-carbanak-hacking-group-behind-a-string-of-big-breaches/
49) Russian GRU agents caught 'hacking' into global chemical weapons watchdog investigating Salisbury – Steven Swinford, 2018, Available at: https://www.telegraph.co.uk/news/2018/10/04/russian-gru-operatives-caught-hacking-chemical-weapons-watchdog/
50) Doctrine for Cybersecurity - Deirdre K. Mulligan and Fred B. Schneider, 2011 Available at: https://www.cs.cornell.edu/fbs/publications/publicCybersecDaed.pdf
51) H. Nissenbaum, Where Computer Security Meets National Security. Ethics and Information Technology, Vol. 7, No. 2, June 2005, 61-73.
52) The Hacked World Order: Elements of Cyber Power - Adam Segal, Council on Foreign Relations, 2016, Available at: https://www.cfr.org/blog/hacked-world-order-elements-cyber-power
53) Ibid.
54) The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age – PublicAffairs Publishing, 2016
55) In Search of India's Cyber Security Doctrine – Dr Omar Anas Policy Brief, 5 June 2015, Indian Council of World Affairs New Delhi, Available at https://www.academia.edu/12881921/In_Search_of_Indias_Cyber_Security_Doctrine_Policy_Brief_5_June_2015_Indian_Council_of_World_Affairs_New_Delhi
56) Cyber-attacks become number 1 business risk – Nick Ismail, 2018, Available at: https://www.information-age.com/cyber-attacks-number-1-business-risk-123471046/
57) Proactive Defense: Understanding the 4 Main Threat Actor Types – RFSID, 2016, Available at: https://www.recordedfuture.com/threat-actor-types/
58) The Anonymous Group: What is it and How big is it – Ali Raza, 2016, Available at: https://www.hackread.com/anonymous-group-what-is-it-and-how-big-is-it/
59) State-Sponsored Cyber Attacks - Paul Pratley, 2015, Available at: https://www.mwrinfosecurity.com/our-thinking/state-sponsored-cyber-attacks/
60) NATO pressing forward on cyber defense, official says – Morgan Chalfant, 2017, Available at: https://thehill.com/policy/cybersecurity/359014-nato-pressing-forward-on-cyber-defense-official-says
61) Available at: https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/
62) In Search of India's Cyber Security Doctrine – Dr Omar Anas Policy Brief, 5 June 2015, Indian Council of World Affairs New Delhi, Available at https://www.academia.edu/12881921/In_Search_of_Indias_Cyber_Security_Doctrine_Policy_Brief_5_June_2015_Indian_Council_of_World_Affairs_New_Delhi
63) Arquilla, John. "Cyberwar Is Already Upon Us." Foreign Policy. N.p., 27 Feb. 2012. Web. Available at: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us
64) Gen. Michael Hayden: Overclassification of Cyber Threats Puts Businesses at Risk – Adam Janovsky, 2018, Available at: https://www.wsj.com/articles/gen-michael-hayden-overclassification-of-cyber-threats-puts-businesses-at-risk-1541018014
65) Crafting the Nuclear Regime Complex (1950–1975): Dynamics of Harmonization of Opaque Treaty Rules -Grégoire Mallard, 2014, Available at: https://academic.oup.com/ejil/article/25/2/445/406216

Dr. Langweg 3, 2410 Hainburg/Donau
Tel. +43 (1) 3583080
E-Mail: office@aies.at
Website: www.aies.at

Layout: Medienbüro Meyer