Michael Zinkanell, David Kirsch

AUSTRIA INSTITUT FÜR EUROPA- UND SICHERHEITSPOLITIK

FOKUS | 4/2021

The Disruptive Impact of the Cyber Domain on International Security Policy

Introduction

Every second, 127 new devices are accessing the world wide web for the first time, while estimates suggest that the total number of appliances connected to the internet, including cars, fridges, smartphones, and watches, amounted to more than 31 billion in late 2020.[1] The global data chain of the internet grows by 2,500,000,000 GB daily.[2] The evolution of information technology not only contributes to an innovative way of work and life, igniting the digital transformation of businesses, but also triggers new wide-ranging challenges for security policy. What started with the invention of the telegraph in 1844[3], the numerical computer in 1949, and the first version of the internet initially launched by the US Department of Defense in 1969, which was subsequently called ARPANET in 1983[4], has indeed caused new strategic implications for the nation state on a remarkable scale.[5] Today, the advancement of digital technologies affects various political systems and stakeholders around the globe, as the dependency on and influence of digitalisation are omnipresent and directly connected to economic growth as well as decision-making processes. Additionally, the growing importance and sophistication of *cyber-warfare* as well as conflicts being conducted in the cyber-sphere continue to produce unprecedented novel dilemmas and security challenges for the security establishment.

This analysis seeks to shed light on various selected and highly relevant difficulties related to the issues of cyber diplomacy, hybrid warfare, and international relations. The authors will briefly depict a short definition of what is and what is not *cyber* by drawing parallels between common cyber conflicts and regular conventional disputes. Subsequently, the authors aim to illustrate how the cyber domain has fundamentally challenged national and international security policy. Finally, there will be a short outlook on the current challenges in the cyber-sphere that are being amplified by the ongoing Covid-19 pandemic – causing severe headache within the security establishment.

Why cyber does not have to be a recipe for catastrophe

Most prominent research on the emergence of information technology and its mutual influence on international politics has a tendency to produce dystopian forecasts[6] about a digital world war.[7] However, reality is much more complex – especially when it comes to security investigators responsible for the attribution of suspects in the cyber-sphere. Regardless of whether looking at regular conflicts or irregular terrorist activities, researchers have been focusing on monitoring perpetrators to gain more information about their motives or potential accomplices. While it is already challenging to monitor terrorist groups in conventional conflicts, the issue of tracking down cyber weapons is even more complex.

The digitalisation of warfare has not only helped to improve already sophisticated defence mechanisms, but has also made digital applications being used as weapons as easily accessible as conventional rifles and handguns. Digital means of cyber operations might either be used for civilian purposes (e.g. to chat and share information via social media), or as a weapon i.e. in disinformation operations.[8] Virtually every cyber weapon consists of code[9], meaning that these programmes are easily and independently producible. This circumstance is facilitating a quasi unrestrained accessibility of malicious cyber instruments, making them widely available for everyone who is equipped with sufficient IT-knowledge that can be self-taught without substantial efforts. Being almost unrestrictedly available in the digital realm, these applications serve as the ultimate low threshold to any cyber conflict.

With regards to conventional conflicts or crime, the issue of investigating and tracking down the financial flows that enabled perpetrators to perform their operations can hardly be overestimated. However, security investigators are mostly aware of the price of ammunition and rifles and might therefore be able to extrapolate potential payments by fellow supporters. On the other hand, when it comes to applications used in the digital realm, the exact cost of cyber-weapons[10] is still unknown.[11] Thus, contrary to the purchase of conventional weapons i.e. in the context of organised crime or terrorism, cyber weapons are much more difficult to be detected and can hardly be regulated, hampering prevention efforts and forensics. In stark contrast to conventional explosives[12], the preparation phase of a cyber weapon is much easier to hide from the prying eyes of security personnel and surveillance cameras. The setup of cyberattacks creates little noise and has meanwhile become very cheap. Attacks that could cost up to $100,000 some years ago can now be conducted by professional actors for as little as $1,000[13], widening the availability of the cyber weapon arsenal, which also opens ways to inexpensively outsource the execution of attacks. Since cyber threat actors are getting more sophisticated per the hour, most experts suggest that there are many processes that will make cyber weapons even more accessible in the near future. Factors include the standardisation of malware development processes and toolkits, as well as the recycling of already existing damaging software. Even though the manufacturing process requires continuous improvement, the learning curve effects of offensive cyber weapons is extremely steep. Additionally, the lack

of scientific and globally recognised consensus on a definition of cyber weapons makes it nearly impossible to distinguish a malicious programme from basic digital applications serving a peaceful and non-threatening purpose.[14]

Yet another key characteristic of the digital reality is the absence of geographic boundaries – unlike any other type of conventional or asymmetric form of aggression, cyberattacks only follow the rules of electronics and are not bound to physical space. Given the global availability of the internet, it is the universal reach of digital applications erasing the necessity of physical presence to conduct warfare. Not only have cyber technologies made it easier to conduct intentionally harmful and aggressive actions underneath the threshold of warfare, avoiding attribution or direct penalisation, they have consequently also dramatically changed the rules of the international power competition. Be it the hacking group linked to an antagonistic or hostile nation state[15] or the 20-year-old lone wolf in his parents' basement[16]: Cyber-technologies made the feasibility of cyberattacks and digital conflicts more proactively viable – hence available for everyone – and enabled threat actors to conduct digital warfare completely remote – e.g. through the heavy usage of *Virtual Private Networks* (VPNs). "The primary benefit to the offense of the cyber domain is the lack of physicality."[17]

Whereas attributing the source of a terrorist attack by conventional means is possible, "attribution is arguably nearly impossible or considered impracticable in the case of attacks carried out via cyberspace."[18] Unlike the construction of regular weapons, cyberspace imposes only few limitations on the construction of major cyber offensive capabilities. The diffusion of reach and power to the individual level not only blurs the line between soldier, civilian, combatant, and non-combatant, but additionally enables non-state actors to cause significant harm without being under steadfast supervision or regulation of a government. That is one of the major reasons, why authoritarian leaders fear relatively unregulated and open technologies like the internet, which might be used as a means to subvert the autocratic political discourse through hidden platforms of communication and exchange. To prevent any unwanted outside information from getting into the virtually closed system, many authoritarian governments i.e. Iran, Russia or China have therefore started building up a state-owned "National Internet".[19] Reza Taghipour, Iran's former Minister of Information and Communication Technology (ICT), equalled unregulated internet access with "buying one's locks from the thief".[20] Until today, Iran has developed into one of the "most sophisticated nations in online censoring" as Iran's leaders try to promote "its national Internet as a cost-saving measure for consumers and as a way to uphold Islamic moral."[21]

While much research has been conducted on the constitution of relationships between minor powers or rebel groups, often acting as proxies for more powerful states[22], the evolution of digital means has steadfastly changed the balance of power between the state and non-state actors in the cyber sphere and tipped it in favour of the latter. To evade attribution and judicial prosecution, more and more states outsource their cyber capabilities into the private sphere to a network of informal actors – sometimes cyber-activists or hacker groups, sometimes even legitimate cyber tech firms. "Resorting to this tactic, it allows cyber threat actors in the state to create plausible deniability and lower the costs (including in reputational terms) and risks entailed by controversial overseas operations."[23]

The sheer possibility of going underground and invisible before and after the conduction of a cyberattack poses serious challenges for security investigators, relentlessly trying to figure out whether a cyberattack was sponsored by the government from whose territory it originated. This so-called *problem of attribution* provides two intertwined challenges for security investigations. First, the technical sophistication of detecting the true origin of a particular attack and second, the identity of those who carried it out, given the boundlessness and anonymity of the cyber domain. More or less akin to regular crime investigations, the challenging process of attribution in cybersecurity resembles those of a judicial evidence process.[24] Cybersecurity forensic experts are required to look for certain pieces of the attacker's identity, parts and traces of which the cyber threat actor might have left on his way of intrusion. To understand the implication of a cyberattack on the security investigators work, one ought to visualise the technical process of a cyber operation, the so-called *kill-chain*, which serves as a model of the path "that an intruder takes to penetrate information systems over time to execute an attack on the target."[25] Most commonly, there are two pieces of action, characteristically shaping the process of a successful cyberattack: "Access" and "Payload".[26] Even before a cyber threat actor manages to successfully access an application, the assailant needs to gain information about the selected victim – e.g. by creating honey-pots which serve as traps. Social Engineering tactics can be additionally used to gain valuable information.[27] While both aforementioned processes do not necessarily leave traces, the moment of digital intrusion most certainly will. After the attacker remotely gained access to the device, the injection of the payload into the machine follows. Sometimes even time stamps being used in the source code serve as valuable meta-information on the equipment being used by the cyber attacker or on the origins of the malware.[28],[29] This meta-data consists of IP-addresses or other registry information and can serve as valuable hints leading to the origin of the attack. After the malicious code has successfully been entered into the victim's system, the cyber threat actor is obliged to communicate with command-and-control servers to move inside the infiltrated networks. Due to the possibility of using various techniques to obscure someone's true location and routing information through multiple machines in various locations across the world, the process of cyber-attribution is highly sophisticated and challenging.

This high level of encryption not only heightens the risk of false attribution, but also – given the lack of a global framework

on cyber-warfare – could lead to serious conflict escalation if a state mistakenly targets an innocent third cyber actor through so-called hack-backs.[30] Until the present day, there is neither a framework to attribute cyberattacks technically, nor judicially. To depict the sheer lawlessness of the cyber-sphere, it is helpful to investigate the policy recommendations of Estonia's former Prime Minister Andrus Antip. In the year of 2007 – after Estonia fell victim to various cyberattacks allegedly financed by and attributed to Russia – he suggested to pre-emptively attribute cyberattacks to possibly (!) involved hackers without any tangible evidence, in order to deter potential actors from future cyberattacks.[31] This "international blame game"[32] could very much turn any investigation into a game of Russian roulette. Indeed, these illustrations genuinely visualise that the world of defensive and offensive cyber actions, cyber-crime, cyber-terrorism, and cyber-warfare is "truly a wild, unruly, and ungoverned place"[33] for policymakers.

It is not new that conventional terrorism seeks to spread fear throughout the entire population of the targeted country, or indirectly inspire more people to join a certain cause by provoking a hostile response or an over-reaction from the affected entity. Terrorism commonly aims at the heart of a society, whose resilience to counter irregular, asymmetric hybrid threats, namely its ability to return to an orderly and normal condition after the occurrence of a tragic event, is vital for its survival.[34] When it comes to cyber, the persistence of a healthy society necessitates a functioning state, whose resilience lies in the functionality of its so-called critical infrastructure (CI). Since the CI serves as a vital area of activity for state and society, be it economy, science, finance, health, telecommunication, electricity or food supply, most cyber threat actors aim to directly inflict damage on critical infrastructure as well as on the state's ability to govern. Due to increased digital interconnectedness, cyberattacks on various elements of critical infrastructure and the consequential cascading effects on the balance of the socio-political system can be described as modern ways to sow widespread discord, fear, and panic. Ultimately, they have the potential to directly endanger people's lives, as the 2013 cyberattack on a water dam in New York clearly showed, in which an allegedly Iranian hacker group hacked an old cellular modem and broke into the command and control system of the dam. Only because the gate had been manually disconnected for maintenance at the time of the intrusion, the attacker was not able to release water from the dam through his remote access.[35] Since this particular element of the U.S. critical infrastructure was poorly safeguarded, with its own networks severely outdated, it consequently posed a serious opportunity for cyber threat actors to exploit the systems' vulnerability, endangering public safety, security, and stability. This could have been the cheapest way to sow panic, while possibly threatening the lives of thousands of New Yorkers. Only three years after the cyberattack, the Assistant Attorney General was able to unveil charges against seven Iranians, who allegedly acted as members of the Iranian Revolutionary Guards Corps.[36] Since the cyber attackers never needed to be physically present to remotely gain access to the dam and operated from a far distance, "there is next to no chance the Iranians will end up in U.S. courts."[37]

Developments in the cybersecurity domain in the context of Covid-19

The most recent developments regarding the growing danger of cyberattacks indicate that not only the tactics, strategies, and technical resources of digitally inflicted harm have rapidly intensified, but also that the amount of attacks has skyrocketed to an unprecedented number of incidents. In the course of the global Covid-19 pandemic, digital attacks – from email phishing to ransomware – against companies, individuals, and state institutions have increased dramatically, as stated in reports by Interpol[38] and the European Union Agency for Cybersecurity (ENISA).[39] The lockdown measures and their consequential shift to working from home demanded for accessing the internet through private and hence often less secure connections. This situation is regarded as the main reason why cybercrime has risen by 75% in the United States in mid 2020 compared to 2019, according to the Federal Bureau of Investigation.[40] Also in Europe it became evident that malicious actors are exploiting digital vulnerabilities, which are enhanced by the pandemic, involving tactics like phishing or the spread of disinformation in seeking to lure victims to fall for online scams.[41]

The general social uncertainties and collective fears inflicted by the pandemic, mixed with financial and economic hardships, are systematically being taken advantage of by all kinds of cyber threat actors: individuals, groups, and states. In addition to the ever more intense personal, commercial, and governmental dependency on digital goods and services, the Covid-19 pandemic has also amplified the reliance on critical infrastructure and the provision of public services. The development and distribution of Covid-19 vaccines, the worldwide strive towards a silver bullet to end the crisis, has transformed vaccination formulas as well as its supply chains into a new critical infrastructure of global scale. However, in return these processes and the value of such crucial knowledge have attracted hackers and criminals alike. According to investigations conducted by IBM[42], the cooling chains required to preserve the Covid-19 vaccine of a public private partnership came under attack from a sophisticated cyber operation, expected to originate from a national aggressor. The cunning attack, targeting six countries and aiming at various key units and organs of the European Commission, followed two parallel objectives. First, the assailant was aspiring to extract and steal sensitive information that could serve as an advantage in the vaccination race. Second, the attack could exploit the weakest links of the digital systems, directly interrupting the supply and distribution chains of vaccines, and ultimately harming the opponents' health care systems. Hence, this malicious tactic can be seen as a dual approach to cause systematic disruption, gaining critical data through cyber espionage, and ultimately endangering human lives.[43] As it is the case in the majority of cyberattacks, no responsible threat actor has yet been publicly identified.

Already before cyber threats became a more potent security risk in the course of the Covid-19 pandemic, the European Union reacted to the growing insecurity by introducing a range of preventative measures and awareness raising initiatives. In order to compressively address the rising and evolving challenges of cyberspace, the European Council in 2019 extended their existing framework to mitigate external threats to the EU and its member states. For the first time, the new European sanction regime allows to execute responsive countermeasures, "including cyber-attacks against third States or international organisations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP)".[44] This action changes the European approach towards cybersecurity both symbolically and practically. Not only are the new measures limiting the potential scope and damage of cyber aggressions against the EU and its members by imposing the option of waging counterattacks, but they are also sending a clear sign. On the one side, the ability to launch concrete defensive measures could have a preventive and deterrent effect on attackers. On the other side, which is even more relevant in the long-term, cybersecurity does not remain simply an abstract and hypothetical concept but becomes a tangible and real risk linked to the common European foreign and security policy. The protection against cyber aggressions and digital threats is not an exclusive national imperative anymore, but rather a shared European responsibility, which is strengthening the cohesion and integration within the EU. An attack on one European member state becomes an attack on all.

Conclusion

Cyberattacks and digital threats will continue to intensify, increase and evolve in the years to come. Online tools and programmes as means of coercion designed to exercise pressure and to cause socio-political or economic disruptions are more available and accessible than ever before. At the same time, the digital interconnectivity between electronic devices is enormously expanding, a development which will be further accelerated by the emergence of the Internet of Things. Thus, both the digital vulnerability of individuals, companies, and states as well as the weapon arsenal of cyberspace are simultaneously growing. Aggressors are expected to proceed weaponising digital technologies as an attractive unconventional means to destabilise opponents.

The sooner the cyber domain is widely recognised as a dangerous security environment, the better it will be included in the perception and assessment of common threats. In order to keep up with the speed of technological advancement, European stakeholders and decision-makers are well advised to fully integrate cybersecurity into their security and defence strategies and frameworks. However, this process should not only involve mechanisms to detect and fend off cyberattacks, but it additionally has to emphasise the bigger picture: Cyber threats are merely one component belonging to a wider spectrum of hybrid, nonconventional, and interlaced forms of aggression, which are skilfully disguised and well-coordinated. Against this background, one crucial future technological advancement to carefully scrutinise is the potential of artificial intelligence in cyber space. Mixed with a growing internationally unstable digital security atmosphere, future breakthroughs in automation and machine learning abilities could intensify the nature of cyber conflicts to yet unknown dimensions. The EU and national stakeholders thus need to take more coordinated and forward-looking actions to fully take the wider range of cyber opportunities and risks into account.

Authors

Michael Zinkanell, MA, AIES Deputy Director

David Kirsch, MA in War & Conflict Studies & certificates in Blockchain (UniHongkong) & Business (LSE London) & IT (Google), currently working as Data Manager at the Health Department of the City of Vienna, focussing on Data Mining, operation efficiency & IT-Operations with regard to the Corona Crisis.

Endnotes

1) Maayan, Gilad David, 2020: "The IoT Rundown For 2020: Stats, Risks, and Solutions", https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx
2) Singer, P.W./Friedman, Allan, 2014: "Cybersecurity and Cyberwar", University Press. Oxford
3) Even, Shmuel, Simon-Tov, David, 2012: "Cyber Warfare: Concepts and Strategic Trends", Institute for National Security Studies, p. 9, http://www.inss.org.il/publication/cyber-warfare-concepts-and-strategictrends/
4) Singer, P.W./Friedman, Allan, 2014: "Cybersecurity and Cyberwar", University Press. Oxford, p. 18.
5) Herpig, Sven, 2016: "Anti-War and the Cyber Triangle. Strategic Implications of Cyber Operations and Cybersecurity for the State", Hull University. https://www.stiftung-nv.de/de/publikation/anti-war-and-cyber-triangle-strategic-implicationscyber-operations-and-cyber-security
6) Carr, Jeffrey, 2013: "Cyberweapons as new WMDs", Bulletin of the Atomic Scientists 69(5) 32–37, https://journals.sagepub.com/doi/pdf/10.1177/0096340213501373
7) Rid, Thomas, 2012: "Cyber War Will Not Take Place" Journal of Strategic Studies Volume 35, 2012, Issue 1 https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939?journalCode=fjss20
8) Select Committee on Intelligence United States Senate, 2019: "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views", https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
9) Herpig, Sven, 2016: "Anti-War and the Cyber Triangle. Strategic Implications of Cyber Operations and Cybersecurity for the State", Hull University, p.6, https://www.stiftung-nv.de/de/publikation/anti-war-and-cyber-triangle-strategic-implicationscyber-operations-and-cyber-security
10) Mele, Stefano, 2014: "Legal Considerations on Cyber-Weapons and Their Definition", Journal of Law & Cyber Warfare, Vol. 3, No. 1 (Spring 2014), pp. 52-69, Published By: Lexeprint, Inc. https://www.jstor.org/stable/26432559?seq=1
11) Council of Foreign Relations, 2016: "How Much Does a Cyber Weapon Cost? Nobody Knows" Blog Post by Guest Blogger for Net Politics, November 21, 2016, https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows
12) Davis, Christina, 2020: "Science in War: How to Make IED" https://topclassactions.com/lawsuit-settlements/military/how-make-ied-bomb/
13) The Wall Street Journal, 2020: "Hackers Eye Their Next Targets, From Schools to Cars", Oct. 8, 2020, https://www.wsj.com/articles/hackers-eye-their-next-targets-from-schools-to-cars-11602169373
14) Infosec, 2012: "The Rise of Cyber Weapons and Relative Impact on Cyberspace" October 5, 2012, Pierluigi Paganini, https://resources.infosecinstitute.com/topic/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/
15) Alperovich, Dmitri, 2016: "Bears in the Midst: Intrusion into the Democratic National Committee", Crowdstrike, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
16) Eddy, Melissa, 2019: "German Man Confesses to Hacking Politicians' Data, Officials Say", New York Times, accessed, March 16 2019, https://www.nytimes.com/2019/01/08/world/europe/germany-hacking-arrest.html
17) U.S. Naval Institute, 2016: "Cyber Weapons Are Not Created Equal", By Captain Christopher A. Bartos, U.S. Marine Corps, Vol. 142/6/1,360, https://www.usni.org/magazines/proceedings/2016/june/cyber-weapons-are-not-created-equal
18) Reinhold, Thomas / Herpig, Sven, 2018: "Credible attribution and Russian operations in cyberspace", Chaillot Paper No 148 des European Union Institute for Security Studies (EUISS) 23. Oktober 2018, https://www.stiftung-nv.de/de/publikation/credible-attribution-and-russian-operations-cyberspace
19) Anderson, Collin / Sadjadpour, Karim, 2018: "Iran's Cyber Threat – Espionage, Sabotage, and Revenge", Carnegie Endowment for International Peace, https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf
20) Khashayar Nouri, 2010: "Tehran's Unplugged Internet Plan", Payvand, October 23 2010, http://www.payvand.com/news/10/oct/1189.html
21) Rhoads, Christopher / Fassihi, Farnaz, 2011: "Iran Vows to Unplug Internet", Wall Street Journal, May 28 2011, https://www.wsj.com/articles/SB10001424052748704889404576273914490020 16
22) Moghadam, Assaf / Wyss, Michel, 2018: "Five Myths about Sponsor-Proxy Relationships" https://www.lawfareblog.com/five-myths-about-sponsor-proxy-relationships
23) EUISS, 2018: "Hacks, leaks and disruptions Russian cyber strategies", CHAILLOT PAPERS No. 148, October 2018, p.15ff, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf
24) Biselli, Anna, 2019: "Attribution ist wie ein Indizienprozess", https://www.golem.de/news/cyberangriffe-attribution-ist-wie-ein-indizienprozess-1910-143527.html
25) Yadva, Tarun / Mallari, Rao Arvind, 2015: "Technical Aspects of Cyber Kill Chain", Third International Symposium on Security in Computing and Communications (SSCC'15), Volume: 536 https://www.researchgate.net/publication/281148852_Technical_Aspects_of_Cyber_Kill_Chain
26) Lin, Herbert, 2016: "Attribution of Malicious Cyber Incidents – From Soup to Nuts", Hoover Institution, https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf
27) Keyworth Marie, 2016: "Vishing and smishing: The rise of social engineering fraud" BBC, 1 January 2016 https://www.bbc.com/news/business-35201188
28) Koen, Renico / Olivier, Martin S., 2008: "The Use of File Timestamps in Digital Forensics", in "Proceedings of the ISSA 2008 Innovative Minds Conference", H. S. Venter, M. M. Eloff, J. H. P. Eloff, and L. Labuschagne (eds.), Johannesburg, South Africa, http://martinolivier.com/open/timestamps.pdf
29) Tanriverdi, Hakan, 2017: "Was der Code russischer Elite-Hacker verrät", Süddeutsche Zeitung, 15.02.2017, https://www.sueddeutsche.de/digital/it-sicherheit-was-der-code-russischer-elite-hacker-verraet-1.3379915
30) Finlay, Lorraine / Payne Christian, 2019: "The attribution problem and cyber armed attacks", The University of Notre Dame Australia, School of Law, Law Papers and Journal Articles, https://researchonline.nd.edu.au/cgi/viewcontent.cgi?article=1089&context=law_article
31) Stupp, Catherine, 2018: "Commission urges EU countries to publicly blame states behind cyber attacks", EURACTIV, https://www.euractiv.com/section/defence-and-security/news/commission-urges-eu-countriesto-publicly-blame-states-behind-cyber-attacks/
32) Bershidsky, Leonid, 2017: "The Cyber Whodunit and the International Blame Game", Bloomberg Opinion, December 19, 2017, https://www.bloomberg.com/opinion/articles/2017-12-19/the-cyber-whodunit-and-the-international-blame-game
33) Tohn, David, 2009: "Digital trench warfare", The Boston Globe, June 11, 2009, http://archive.boston.com/bostonglobe/editorial_opinion/oped/articles/2009/06/11/digital_trench_warfare/
34) Jore, Sissel, H., 2020: "Is Resilience a Good Concept in Terrorism Research? A Conceptual Adequacy Analysis of Terrorism Resilience" https://www.tandfonline.com/doi/full/10.1080/1057610X.2020.1738681
35) Thompson, Mark, 2016: "Iranian Cyber Attack on New York Dam Shows Future of War", TIME USA LLC, March 24, 2016, https://time.com/4270728/iran-cyber-attack-dam-fbi/
36) U.S. Department of Justice, 2016: "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector", Department of Justice, Office of Public Affairs, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged
37) Thompson, Mark, 2016: "Iranian Cyber Attack on New York Dam Shows Future of War", TIME USA LLC, March 24, 2016, https://time.com/4270728/iran-cyber-attack-dam-fbi/
38) Interpol, 2020: "COVID-19 cyberthreats", https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
39) European Union Agency for Cybersecurity (ENISA), 2020: "Understanding and dealing with phishing during the COVID-19 pandemic", May 06, 2020, https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic
40) The Economist, 2020: "During the pandemic a digital crimewave has flooded the internet" https://www.economist.com/international/2020/08/17/during-the-pandemic-a-digital-crimewave-has-flooded-the-internet
41) Europol, 2020: "Covid-19 Sparks Upward Trend in Cybercrime", 05 October 2020, https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime
42) Sanger, David E. / LaFraniere, Sharon, 2020: "Cyberattacks Discovered on Vaccine Distribution Operations" New York Times, 14 December, 2020, https://www.nytimes.com/2020/12/03/us/politics/vaccine-cyberattacks.html
43) Kuchler, Hannah / Murphy, Hannah, 2020: "Covid vaccine supply chain targeted by hackers, say security experts", Financial Times, 03 December, 2020 https://www.ft.com/content/9c303207-8f4a-42b7-b0e4-cf421f036b2f
44) Council of the European Union, "Cyber-attacks: Council is now able to impose sanctions", Press Release, 17 May, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

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

Layout: Medienbüro Meyer