2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

The Cyber Decade: Cyber Defence at a X-ing Point

Robert Koch
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany
robert.koch@unibw.de

Mario Golling
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany
mario.golling@unibw.de

Abstract: As a consequence of the numerous cyber attacks over the last decade, both the consideration and use of cyberspace has fundamentally changed, and will continue to evolve. Military forces all over the world have come to value the new role of cyberspace in warfare, building up cyber commands, and establishing new capabilities. Integral to such capabilities is that military forces fundamentally depend on the rapid exchange of information in order for their decision-making processes to gain superiority on the battlefield; this compounds the need to develop network-enabled capabilities to realize network-centric warfare. This triangle of cyber offense, cyber defence, and cyber dependence creates a challenging and complex system of interdependencies. Alongside, while numerous technologies have not improved cyber security significantly, this may change with upcoming new concepts and systems, like decentralized ledger technologies (Blockchains) or quantum-secured communication.

Following these thoughts, the paper analyses the development of both cyber threats and defence capabilities during the past 10 years, evaluates the current situation and gives recommendations for improvements. To this end, the paper is structured as follows: first, general conditions for military forces with respect to "cyber" are described, including an analysis of the most likely courses of action of the West and their seemingly traditional adversary in the East, Russia. The overview includes a discussion of the usefulness of the measures and an overview of upcoming technologies critical for cyber security. Finally, requirements and recommendations for the further development of cyber defence are briefly covered.

Keywords: *cyber war review, cyber defence implications, cyber defence recommendations, cyber defence requirements, future technologies, cyber war*

1. INTRODUCTION

As a consequence of the cyber attacks on Estonia in 2007, both the consideration and use of cyberspace by the military has fundamentally changed and will continue to do so. Over the years, such attacks have effectively demonstrated how significant impacts can be wrought by supposedly trivial and low-key means. On the other hand, military forces also depend strongly on the rapid exchange of information for their decision-making process so their forces can gain battlefield superiority, which enforces the need for network-enabled capabilities (NEC) [1] to realize network-centric warfare (NCW) [2]. This creates a challenging and complex system of interdependencies, opening a broad spectrum of possible attack vectors. Therefore, operations in cyberspace can be used to generate effects not only in cyberspace itself, but also in the physical environment, which is an attractive new capability for military commanders. Indeed, armed forces worldwide now highly value the new role of cyber, and are building cyber commands and establishing new operational capabilities, and the asymmetric nature of cyber warfare can give the advantage to armed forces otherwise in possession of comparatively smaller weaponry. However, the complexity of sophisticated cyber attacks like Stuxnet can also imply the opposite. Thus, cyber defence is also of enormous importance. And while numerous technologies proposed over recent years have not improved cyber security significantly, this may change with upcoming new concepts and systems. Blockchains, quantum-secured communication, mathematically verified software microkernels, and trusted hardware platforms are likely to be key elements for new, more secure systems. Along with the armaments industry itself developing a better understanding of cyber threats, this should lead to better and more resilient weapon systems.

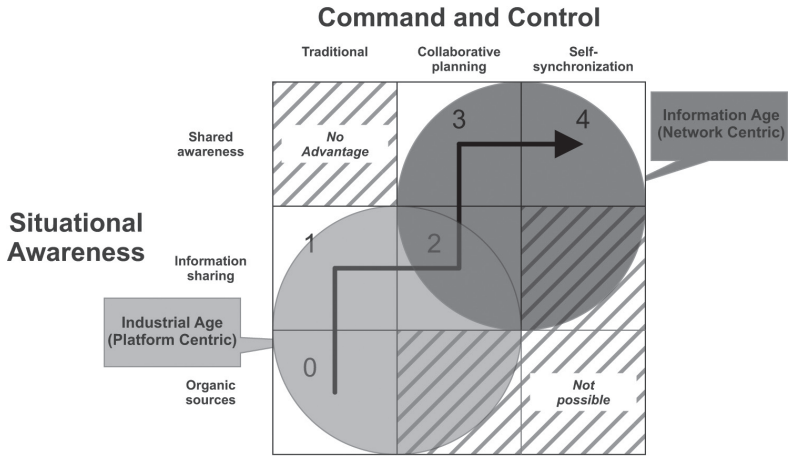
In light of these thoughts, the paper analyses the development of both cyber threats and defence capabilities over the past 10 years from 2007 to 2017, evaluates the current situation and gives recommendations for further development. The paper is structured as follows: first, general conditions for military forces with respect to “cyber” are described and dependencies and requirements are highlighted. Second, a brief overview of the development of cyber threats and defence capabilities during the past ten years is given, including a discussion of the usefulness of the measures. Upcoming technologies which are important for cyber security are briefly discussed to analyse opportunities for more secure systems. Finally, the conclusions of the paper are summarized and requirements for the further development of cyber defence are derived.

2. DETERMINING FACTORS

For all the millennia of warfare that have passed, the tools and tactics of how armies fight have evolved as military technologies have evolved [2]. However, recent years have seen fundamental changes come to affect the very character of war [2]. Military forces worldwide are increasingly capitalizing on the advances and advantages of information technology to facilitate radical changes in the way they structure and deliver offensive and defensive capabilities [1]. The US Navy was among the first to investigate how to use Information and Communication Technology (ICT) to increase the efficiency and efficacy of their forces on the 21st Century battlefield [3], the main consequence being the increased integration of individual, hitherto autonomously acting systems, thus a fundamental shift from what is called platform-centric warfare to network-centric warfare (NCW). NCW harnesses network technology to facilitate radical improvements in the shared awareness of disposition and intent, together with a capability for rapid reconfiguration, and synchronization of operations [1] and thus improves both the efficiency and effectiveness of military operations [4].

As such, NCW creates superiority in war by harvesting information from a network of reconnaissance systems and enabling its analysis and use by command and control centres, as well as use in weapons systems. Hence military superiority across the entire range of military operations, i.e. full spectrum dominance, is achieved. The vision for NCW is to provide seamless access to timely information at every echelon in the military hierarchy and enable all elements to share information within a single, coherent, complete, and dynamically accurate picture of the battlefield. It is intended that NCW will produce an improved understanding both of the intent of higher command and of the operational situation at all levels of command, with every element better able to tap into the collective knowledge and reduce the “fog and friction” [4] of war, and enable the optimal use of resources. Although the transformation towards NCW is not finalized completely, even not by the United States [1, 4], NCW is anticipated to be one of the greatest revolutions in military operations in the past 200 years (see Figure 1).

FIGURE 1. NCW ROUTE MAP [5, 6]



However, within such an integrated system lies a greater vulnerability: attacking the weakest link could compromise the entire system and lead to catastrophic consequences, in the worst case rendering an entire military force incapable of action.

A. On Multinational Coalitions

In addition to the increased use of information technology, the aspect of cooperative, multinational participation in conflicts is of great importance. Military operations today are almost always multilateral in complexion. With regard to NATO, since 1990, there has been a significant increase in the number of military operations requiring NATO member states to contribute forces to some multinational coalition or alliance [7]. Moreover, the range of mission types has broadened to include peacekeeping, peace support, and humanitarian operations [7]. Corresponding challenges with such a force are, for example, what the agreed operational concepts are, different intelligence requirements and structures, the diverse capabilities and qualities of the various formations as well as command, control, communication, and intelligence (C4I)/cyber interfaces that have to be developed and integrated [8, 7].

Increased defence cooperation, such as "Smart Defence" (NATO), "Pooling & Sharing" (European Union), or the "Framework Nations Concept", in theory increases sustainability and helps to preserve key military capabilities [9]. Smaller armies can plug their remaining capabilities into an organizational backbone provided by a larger, "framework" nation [9]. In practice, however, this theory has yet to fully prove itself, and the extent to which those well-understood obstacles to defence cooperation can be overcome remains to be seen [9, 10]. Deeper cooperation also calls for reliability among the different partners [9]. In terms of ICT, cyber is always a potential risk.

Therefore, it can be said that despite the undisputed advantages of multi-national coalitions, a military force made up of numerous divergent parts can see the overall system's cyber defences be compromised, which can easily play into the hands of the attacker and hamper one's own defence.

B. On Russia – Analysis of Russia's Course of Action

Western countries follow the assumption that economically prosperous democracies are less likely to wage war against each other. Therefore, the EU operates a "Europeanization policy" aimed at democratization and economic liberalization, particularly in its eastern domain [11]. This basic principle of foreign policy, however, is by no means *a priori* transferable to all states. In light of Russia's annexation of the Crimea in Ukraine and the war in the Donbas, unresolved territorial conflicts on the eastern borders of the EU have gained international attention and concern. From Russia's perspective, the West's approach is flawed on several fronts. In context, shortly after World War Two, the Kremlin sought to protect the USSR by establishing a *cordon sanitaire* between itself and its major nemeses, the Western powers [13], with the occupation and coercive support of eastern European states under the Warsaw Pact. Although this buffer zone disintegrated over 1989-1991, as did the USSR itself, with the Kremlin believing its borderlands could slip under the aegis and control of the West, Moscow created the concept of "Frozen Conflicts" to weaken, divide, and ultimately prevent these countries (Moldova, Georgia, and Ukraine, for example) from drifting far from their eastern orbit of Russia [13]. Russia did so through the manipulation of nationalist impulses among border populations [13], encouraging minorities to think of themselves as distinct from the majority population [13]. Unwilling to risk more than limited open military intervention, the Russians enhanced hybrid warfare (which has its origins in 1938), using the presence of its peacekeepers and its diplomatic powers to keep these conflicts in a "no war, no peace" situation (i.e., Frozen Conflicts) that perpetuates a Russian role in its borderlands [13].

As much as Russia profits more from enabling if not inciting temporary and regionally-limited "skirmishes" to justify its own intervention, it is important to prevent the West from being drawn into these conflicts. Hence the importance of the concept of "Escalation Dominance" within every domain, including cyber, which imparts the ability to create a credible deterrence to outside forces involving themselves. Like any offensive or defensive capability, this will only work as a deterrent if the host nation shows it has the appropriate means, and the will to use them. As a conclusion, it can be stated that Russia – unlike the West – benefits more from regionally limited Frozen Conflicts and, for reasons of Escalation Dominance, also in terms of cyber, might feel the need to demonstrate Cyber Dominance to hamper other nations engaged or seeking to engage in those conflicts. Correspondingly, this increases the likelihood of cyber attacks.

3. A DECADE OF CYBER THREATS AND DEFENCE

Making hard decisions in the area of cyber security requires a comprehensive understanding of cyber security threats and developments. What follows then is an analysis of the last 10 years in the evolution of cyber threats and defence from 2007 to 2017, the starting point being the Distributed Denial-of-Service (DDoS) attacks on Estonia, which marked a step-change in the onset of cyber warfare.

A. Development of Security Incidents

CyCon X signifies 10 years of conferences dealing with legal, strategic, conceptual, and technical challenges of cyber conflict. Motivated by the consequences of the DDoS attacks on Estonia [14], which affected broad parts of everyday life in a country that had already highly digitized systems of infrastructure and governance, the conferences sought to explore and discuss numerous aspects of cyber security.

2007-2009: The DDoS attacks on Estonia were not the only remarkable event in 2007. DDoS attacks are themselves a relatively simple method of attack, where vast amounts of data requests are directed towards a target with the aim of exhausting the target's means of providing data, and legitimate traffic is blocked out in a simple but effective method. But this is just one case and while any number of digital assaults may be ostensibly quite primitive in format, it is the failure to anticipate them that enables their effectiveness, and significant, material impacts can be delivered. For example, the US Department of Energy ran the so-called Aurora experiment in their Idaho Labs in 2007 [15], showing how an attack on a power generator's control system could led to the generator's destruction. These incidences, both actual and theoretical, brought the issue of vulnerabilities in modern critical infrastructures into the public domain for the first time.

Meanwhile, a remarkable military operation was undertaken by the Israeli Air Force (IAF). During Operation Orchard, the IAF executed a pre-emptive strike against Syria's plutonium-powered nuclear reactor Al Kibar shortly before it became active [16]. Highly successful, no plane was lost, with not a single Syrian missile fired. Some reports said this was because Syria's air-defence systems were blinded by standard electronic scrambling tools [16], but some analyses highlighted the use of either special software or a backdoor in the adversary's systems as more likely explanations for their failure to fire [17].

The notorious worm Downadup (also known as Conficker) appeared in October 2008. While worm attacks had already been declining for some years, Downadup manifest itself as one of the most widespread threats seen in some time [18]. It combined several techniques to spread itself and hide within systems, and defend itself against

attacks. Even by 2014, over a million machines were still infected, highlighting the difficulties of removing this malware [19]. The ability to observe the defenders and adapt the code underlined the sophistication of the hackers [20]. While attribution of the precise origins of the attack is still not clear, with the creators of Downadup remaining unknown, sources were traced to Ukraine and China. Only the last version of the worm carried a malicious payload and it was a version that deleted itself after a month. This may indicate that Downadup was more of a test run by a still unknown source rather than a directed attack by cyber criminals.

Also in 2008, manipulated credit-card readers were found in UK supermarkets. The devices were fitted with wireless equipment and could transmit stolen data once a day or go dormant to avoid detection [21]. This was a remarkable attack on the country's retail supply chain and its customers.

The rising threat towards critical infrastructures was seen when the US Federal Aviation Administration's computer systems were hacked in 2009 [22], endangering not only commercial air traffic but military operations as well. In February, the (in-) famous Downadup malware together with poor cyber hygiene grounded French naval aircraft [23], and in December, the US military realized that Iraqi insurgents had used the $26 software "SkyGrabber" to capture video feeds from US drones that had been transmitted via satellite links [24]. Despite what newspapers reported at the time, there was no "hacking" involved, only installing the software, aligning the antenna, and starting the record: the transmissions themselves were unencrypted.

2010: Some serious incidents affected the Internet in early 2010. Apparently, a configuration error made the I-root instance of the Domain Name System (DNS) root servers visible outside of China. I-root does not give correct address resolutions for all queries because of online censorship in China. Suddenly it was being used by computers outside of China, which unintentionally fell into this censorship [25]. Only two weeks later, a small Chinese ISP called IDC China Telecommunications Corporation, that had normally sourced about 40 prefixes, announced nearly 37,000 unique prefixes for about 15 minutes. Because of that, approximately 10 per cent of Internet traffic was rerouted through China, including traffic from providers like Deutsche Telekom and AT&T [26]. The incident highlighted how a good understanding of structures and protocols can be used to generate simple and effective attacks.

An important incident was discovered in October 2010 by the Belarusian company VirusBlokAda: Stuxnet. While the complexity of the malware sample challenged the security companies (resulting in some incorrect analysis), eventually it was determined that the malware attacked the Iranian enrichment facility in Natanz, interfering with the enrichment process and finally destroying centrifuges [27]. While it was not, as

reported at the time, the first cyber attack to result in physical damage, it definitely was a game changer, clearly demonstrating the new opportunities thrown up by a globalized, interconnected world. Even more, it marked the start of a new area of cyber ambitions from numerous countries around the world.

2011-2012: A sophisticated spear-phishing attack in 2011 obtained data used to compromise network security company RSA's SecureID technology, which was then used to attack Lockheed Martin [28].

In 2012, the media reported on Chinese hackers stealing classified information about Lockheed Martin's F-35 Joint Strike Fighter (JSF), as revealed by documents obtained by the NSA whistle-blower Edward Snowden (whose own story is a testament to how vast, top-security IT systems can be compromised by one person with a USB-stick, see below) [29]. Comparing Lockheed Martin's JSF and China's Shenyang J-31 fighter, David Majumdar has said: "On the surface, the J-31 looks very much like a twin-engine F-35 clone – and there are plenty of reasons to believe that the Chinese jet was based on stolen JSF technology – and could eventually be more or less a match for the American jet" [30].

Another controversial discussion was about a hardware backdoor in the Microsemi ProASIC3 processor – a chip used in numerous high performance aircraft, ranging from USAF fighters to the Boeing 777 Dreamliner, as well as military applications like encryption devices. While the researchers found some processor commands on-board the chip which could be used as a backdoor [31], industry argued that these functions were only undocumented debugging functionality to be used by the chip developers for testing purposes. On the one hand this may be true, especially as modern processors contain thousands of undocumented commands and features [32], but on the other hand, for a sensitive or classified military application, it was a dangerous attack vector.

2013-2014: The power of relatively simple hacks when executed by an agent with a strong understanding of a system and its dependencies was once again demonstrated in April 2013, when a fake Tweet sent by the Syrian Electronic Army via the Associate Press's Twitter feed caused a temporary crash of the New York Stock Exchange, costing US $136 billion. The content of the tweet said "Breaking: Two Explosions in the White House and Barack Obama is injured" [33]. Of course, it was quickly realized that there had not been an attack and the index recovered quickly; nevertheless, knowing (or executing) such a ploy can result in a lot of money being lost, or at least, changing hands when otherwise it might not.

Another major event that should profoundly change the importance with which cyber security is viewed was the Snowden Leaks. The whistle-blower Edward Snowden worked as a system administrator for the NSA until May 2013. He passed on top secret, classified information about surveillance projects to the world's press. The range of the revelations was vast, from the eavesdropping of Internet links, the introduction of hardware as well as algorithmic backdoors, to techniques for bridging the air-gap [34].

The Snowden Leaks came as part of a growing tide of stories about incidents of high level breaches of data and hacking. Even so, another breach in 2014 is of particular note, with the US Office of Personnel Management (OPM) targeted [35]. The severity of the breach stemmed from the business engaged in by the companies concerned, namely KeyPoint Government Solutions, the contractor for OPM, doing security clearance background investigations. Thus, the nature of the data was highly critical, not only because of personally identifiable information like Social Security numbers and addresses, but because of the risk of interference with and blackmailing potential of actual employees, with information heisted from such background checks.

In October 2012, NATO identified a comprehensive espionage campaign [36] that was attributed to Russia, and was found to have been going for five years already, additionally targeting institutions of the EU and the Ukrainian government. As is often the case, it was very difficult to give a close estimate as to quantity of data stolen. For example, logging data is often available only for short periods of time and is limited by legal regulations, which confounds the chances of getting a complete picture of what has happened. Hence, identifying the extent of the damage, and by that the scale and detail of potential hazards thereafter faced, is highly challenging.

There were also breaches identified and intensified in the energy sectors in the United States and across Europe. Hackers from the "Dragonfly" group, also known as "Energetic Bear", and traced to Eastern Europe, successfully hacked IT systems run by energy grid providers, electricity generation firms, petroleum pipeline operators, and industrial equipment providers in the US, Spain, France, Italy, Germany, Turkey, and Poland [37]. While the primary objectives were espionage and persistent access, there also remained the capability to carry out acts of sabotage [37].

2015: A highly "visible" attack occurred in April 2015, when 12 channels of the broadcasting station TV5 Monde went off air. While a defacement displayed IS propaganda online, an investigation identified the Russian hacker group APT28 as the source of the attack. It was a well-prepared assault and possibly sought to destroy the television station, but greater damage was prevented by the serendipitous presence on site of many more technicians than usual due to a new channel going on air the

same day of the attack [38]. Another attack resulting in actual physical consequences was demonstrated in western Ukraine in December. A long-prepared cyber attack on multiple electricity distribution stations caused power outages that affected approximately 225,000 customers. In parallel, phone DoS attacks were carried out on call centres to prevent customers from contacting the power company under assault [39].

2016: Early 2016 saw the beginning of the end for old-school methods of bank robbing, i.e. masked men with guns telling everyone to get on the floor, as new high-tech methods introduced themselves to the world stage [40]. An attacker group named "Lazarus", traced to North Korea, stole a total of over US $100 million, mainly from the Bangladesh Bank, among others, by penetrating the Alliance Access software used by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) networks, which carries worldwide financial transactions in a (up to that point) secure and standardized way. In the same year, North Korean hackers also looted 235 GB of sensitive documents from South Korea's defence data centre, including blueprints for a joint-US plans for war on the peninsula and scenarios for removing the North Korean leader, Kim Jong-un [41].

During the breach of the Philippines Commission on Elections, personal information from all of the country's 55 million registered voters, including fingerprint data, passport numbers, and expiry dates, was exposed online and fully searchable [42], while the designs of India's Scorpion submarines was leaked from the French shipbuilder DCNS [43]. Other data breaches that came to the public's attention involved the casual dating website AdultFriendFinder, with the details of 412 million users exposed to the world [44], and even the NSA's own hacking tools were stolen by the hacker group "The Shadow Brokers" [45].

But while such incidents have grown in number and severity, the methods deployed in the attacks techniques are still often quite simple, with DDoS attacks achieving disruption of services ranging from Amazon and Netflix to the PlayStation Network – nearly one decade after the attacks on Estonia.

2017: Numerous cyber security incidents were seen in 2017. In May, the WannaCry ransomware campaign hit enterprises and institutions all over the world [47], with impacts including the taking offline of 61 National Health Service hospitals in the UK and leading to production at numerous Renault factories in France stopping. By using the ETERNALBLUE vulnerability stolen from the NSA in 2016 and published by the Shadow Brokers in April 2017, the malware was very virulent. While patches had been made available by Microsoft for supported systems in March 2017, the run affected especially older Windows XP/8/Server 2003 systems for which no patch

had been published. In light of the outbreak, Microsoft took the "extraordinary" and "unusual" step of providing an emergency update for the aforementioned systems [48]. While the attacks elicited little by way of ransom, the financial impact can be enormous. An attack by the NotPetya ransomware later in 2017 on Maersk cost the Danish shipping giant up to US $300 million [49].

Some details about stolen data from the NSA were also published. A contractor for the organization had without authorization copied data and stored it on his computer at home. Russian hackers then compromised that computer and raided the files. According to *The Wall Street Journal*, the files had been identified by the Russian attackers through the contractor's use of a popular antivirus software made by the Russia-based company Kaspersky Lab [50]. In addition that year, a new series of classified documents was leaked, this time from the CIA [51]. The material called Vault 7 and 8 showed the activities of the CIA in detail, including compromising cars, Smart TVs, and smartphones, and the CIA's capability to conduct cyber warfare [52].

Already by this selection of cyber security incidents of the past 10 years, it seems that the situation has not been improving. To better understand the underlying problems, as well as new opportunities for cyber defence, a quick look at security-related developments during the decade in question follows.

Technological Development

Looking back to 2007, the Canadian company D-Wave Systems, Inc. presented their first commercial 16-qubit quantum annealing processor. Annealing is not universal quantum computing (the most powerful form of quantum computing), and is really only able to solve optimization problems. But D-Wave was the first company using quantum effects for building new kinds of processors. A publication in 2015 [53] led to heated debates over the statement that a calculation by an annealing-based system was carried out "100 million times faster than [that of a] PC", but the comparison was not fair; the problem was greatly optimized for that demonstration and only slightly reflected real-world problems. Moreover, it was easy solvable by certain cluster-detecting algorithms, which were not used for comparison in the paper [54]. Anyway, while no application has been found yet where quantum annealing notably outperforms classical simulation approaches, the benefits of quantum annealing are becoming better understood and speed advantages have been demonstrated [55]. Further steps towards a universal quantum computer have been made, e.g., IBM presented a 50-qubit quantum processor in late 2017 [56]. While quantum key distribution (QKD) enables mathematically provable secure connections, and for which commercial systems have been offered since 2003, there have also been attacks on these systems that target weaknesses in their implementation. For example, Liu

and Sauge demonstrated a hack of QKD back in 2009, while the following year Xu et al. demonstrated the "phase remapping" attack.

In 2008, a paper by an author who called himself Satoshi Nakamoto was published, describing a peer-to-peer electronic cash system [57]. While the elements of the concept, cryptographic signatures, Merkle Chains, and P2P-networks, had already been known, the author was able to solve the double-spending problem by combining them within a distributed, trustless consensus system. The further success of Bitcoin is well-known, but the underlying concept of Blockchains is much more powerful, as it is able to guarantee the integrity of arbitrary data and enable different applications in the area of cyber security [58].

In 2009, a search engine well-known among security researchers was founded: Shodan [59]. Unlike previous systems, Shodan scans the Internet for connected devices, looking at services and collecting all provided information [60]. Different techniques for handling data evolved, especially in the area of big data and cognitive systems. For example, IBM celebrated a great success for cognitive systems in 2011, when IBM's Watson computer won the Jeopardy! challenge [61]. Since then, Watson has been deployed in more and more areas, e.g., cancer treatment, financial planning, or advanced cyber threats and defence.

Much progress has also been observed in the area of Artificial Intelligence (AI). Going beyond the search in problem spaces or behaviour-based approaches, AI is opening up more and more fields, in creativity and even in consciousness [62]. For example, AI is already able to paint new art based on original drawings [63], or compose new music [64]. Of course, there have also been hurdles. Microsoft's Twitter chatbot "Tay" had to be shut down in 2016 after less than 24 hours because it began using racist language [65], while a team from MIT's Computer Science and Artificial Intelligence Laboratory tricked Google's AI into misidentifying pictures of turtles as weapons [66]. Nevertheless, the well-disposed AI program Sophia was granted citizenship in Saudi Arabia in 2017. Now, Sophia is calling for women's rights [67]. Also, Google's already well-known AlphaGo AI system was enhanced even further in a very interesting and powerful away, being no longer constrained by the limits of human knowledge, but learning tabula rasa from itself and outperforming all previous systems [68].

From a military perspective, in 2013 the Chief of the General Staff of the Russian Federation Armed Forces, General Valery Gerasimov, published an article highlighting the asymmetrical possibilities offered by cyberspace and the necessity of perfecting activities in this information space [69]. In summary, the approach is guerrilla, and waged on all fronts with a range of actors and tools – for example, hackers, media,

businessmen, leaks and, yes, fake news, as well as conventional and asymmetric military means. Chaos is the strategy the Kremlin pursues, Gerasimov specifies that the objective is to achieve an environment of permanent unrest and conflict within an enemy state [70]. In November 2014, the US Secretary of Defense Chuck Hagel announced the "Defense Innovation Initiative" [71], with the aim being to "pursue innovative ways to sustain and advance our military superiority for the 21st Century" [71]. To stop the erosion of American dominance in key domains in waging war, it is necessary, he argued, to find "new and creative ways to sustain and in some areas expand our advantages even as we deal with more limited resources" [71]. While this sounds quite challenging, it is historically motivated: "The US changed the security landscape in the 1970s and 1980s with networked precision strike, stealth, and surveillance for conventional forces. We will identify a third offset strategy that puts the competitive advantage firmly in the hands of American power projection over the coming decades" [71].

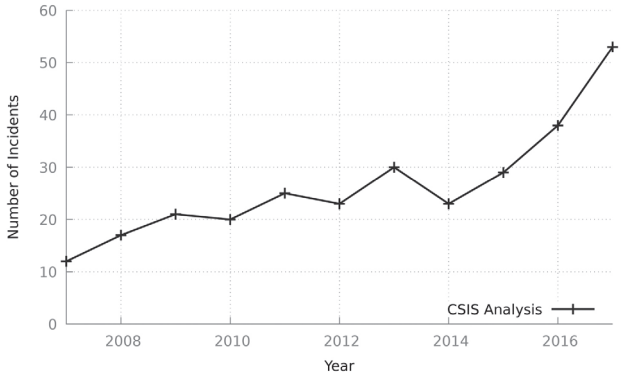
As new and challenging technologies are emerging with increasing pace, many of which are part and parcel of cyber security, a closer look at the root causes of the incidents between 2007-2017 incidents is necessary.

B. Attacker vs. Defender

Today, hundreds of cyber security systems are available on the market. Already back in 2004, the market research company International Data Corporation (IDC) coined the term "Unified Threat Management" (UTM). Basically, UTM is the evolution of firewall techniques into a comprehensive security solution, containing areas like control usage and policy enforcement, and therefore, combining techniques like content filtering, intrusion detection, and prevention, DDoS mitigation and antivirus applications. However, in spite of so broad and extensive an approach to cyber security, cyber security incidents are on the rise in number and gravity. Indeed, as with antivirus software being the conduit for hackers being able to expose data on a NSA contractor's laptop, we are repeatedly seeing how products intended to protect the system have become the gateway for attackers (e.g., see [72]). It is not unsurprising then that in 2015 Netflix chose to discard its antivirus systems [73].

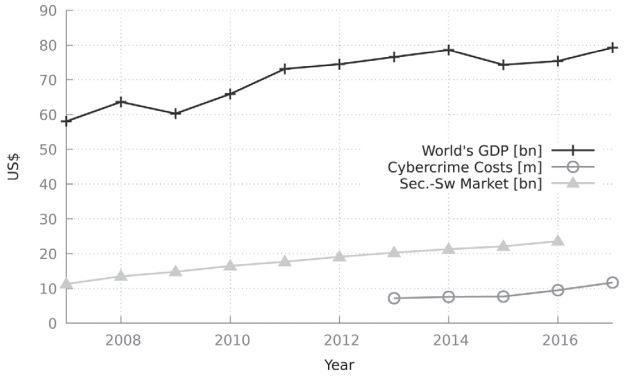
As a definition of an "incident" we should exclude any "ping" or an attempted connection from an unknown machine, as they generate huge numbers, but for the most part are of no greater significance. An attempt was made but failed. Far better then to concentrate on events where huge amounts of personal data or confidential files or even money have been stolen, or where physical damage has been wrought. The Center for Strategic and International Studies (CSIS) has recorded incidents [74], with Figure 2 charting occurrence since 2007.

FIGURE 2. NUMBER OF SIGNIFICANT CYBER INCIDENTS SINCE 2007 AS RECORDED BY CSIS [74]



It is particularly noticeable how the number of significant cyber security incidents has risen since 2015. However, a major variable is the efficacy of protective measures, which can be affected by numerous factors, including falling investment in cyber security. Hence figures for investment in cyber security are included in Figure 3, which shows investment in cyber security has consistently risen [75–77], even in the years of global economic crises when overall GDP has contracted [78].

FIGURE 3. EVOLUTION OF THE GLOBAL GDP, THE CYBER SECURITY MARKET REVENUE AND THE AVERAGE COST OF A CYBER INCIDENT BASED ON [75-78]



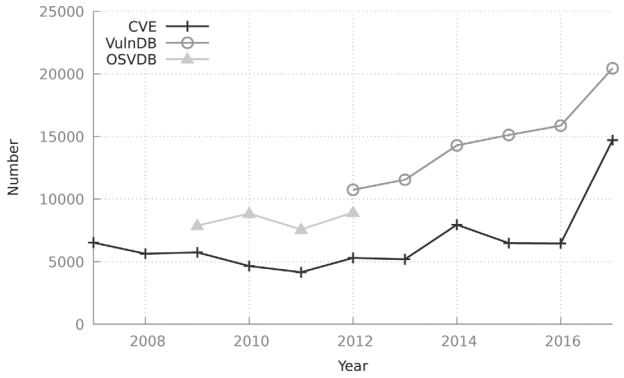
Estimating the net loss generated by cybercrime is a challenging task. Official numbers published by government or non-governmental bodies are a weak indicator, as only those cases filed with them are included. Additional data can be harvested from companies engaging in surveys on the matter, but this may still only be scratching the surface. Various public and private sources produce reports on a regular basis, but even when comparing the same periods under review, there is no consistent picture regarding cyber-attack statistics. For example, IDG's summary of PwC's Global State of Information Security Survey 2018 [79], published on October 18th, 2017, states

that “The number of security incidents detected continues to drop, along with the average financial loss due to cyber security attacks. However, the financial loss per incident continues to climb” [80]. In contrast, the 2017 Cost of Cyber Crime Study published by Accenture on September 26th, 2017, highlights a 27.4% *increase* in the average annual number of security breaches [81]. This underlines how the presented numbers cannot be generalized and how difficult it is to estimate the total damage, with the lack of reliable data being a core issue [82]. Recent studies by McAfee and CSIS throw some light on the subject by estimating the economic impact [83] and the global cost of cybercrime [84]. The most recent report suggests that the global cost of cybercrime is now US $600 billion, which includes gains to criminals and costs to companies for recovery and defence [84]. Within the studies, McAfee highlights the importance to include certain additional indirect costs, such as reputational damage, and this is also emphasized by Anderson et al. [85].

Thus, the global damage has increased sharply since the calculations for the period 2013-2014 where the estimation was US $400 billion [86]. The data is on a par with calculations from the British insurance company Lloyd’s. Anderson ultimately concluded, “that we should perhaps spend less in anticipation of computer crime (on antivirus, firewalls etc.) but we should certainly spend an awful lot more on catching and punishing the perpetrators” [85].

While there are only a few studies dealing with net losses, a large number of cyber security reports are released. For example, Verizon’s Data Breach Investigations Report (DBIR) 2017 indicates that 75% of data breaches are perpetrated by outsiders and 25% involved internal actors [87]. For the tactics used, Verizon surmised that 62% of breaches featured hacking, 51% included malware, and 43% had been social engineering attacks [87]. Still, such numbers are too abstract to identify underlying problems. For example, Figure 4 shows the evolution of known vulnerabilities, as seen by Common Vulnerabilities and Exposures (CVE) [88], Open Sourced Vulnerability Database OSVDB [89], and Vulnerability Database VulnDB respectively [90] (OSVDB was discontinued in 2012, the same year VulnDB started). The range of very different identified vulnerabilities per year is striking. This may be due to some databases also including additional, non-publicly available information in their statistics. As vulnerabilities are the gateway for attackers, one would assume that an evaluation of this data brings light into the cyber security darkness. However, an in-depth analysis by Rory McCune showed that the technical evaluations of various reports are “built on faulty data at best” [91, 92]. As the used data is heavily biased, evaluations are not representative of real-world challenges and by that, are not the strongest of foundations upon which to base any counter action or cyber defence strategies.

FIGURE 4. DEVELOPMENT OF IDENTIFIED VULNERABILITIES AS SEEN BY CVE AND OSVDB/ VULNDB [88-90]



The publicly known vulnerabilities may also be biased [93]: publications strongly depend on the interest and knowledge of some researchers, e.g., the pattern of "local privilege escalation", where vulnerability numbers followed an expected pattern based on the knowledge of researchers and their activities [94]. Therefore, analysing the vulnerability databases is not enough to obtain a comprehensive and accurate picture of the scale of hazards and events encountered.

Overall, then, one can see that neither the array of figures and cases of cyber security breaching incidents, nor the evaluation of vulnerabilities or malign programs, can suffice to comprehensively address all the challenges posed by cyber security issues. Even as investment in cyber security constantly rises, so too are overall net losses growing, and strongly so. An analysis of the root causes is challenging, due to the inherent limits of available data, how it is collated, how incidents are defined, and other flaws and biases innate to any study. All these factors complicate the question then of what is to be done, what kind of effective measures can be deployed in defence. For all of that, efforts need to be made to construct a macro-level investigation of the global situation involving all actors and agents, to best identify the scale of the problems and what can be done about them.

C. Conclusions from 10 Years of Cyber (In)security

Looking back at 10 years of cyber security incidents and technical circumstances and development, a number of trends can be identified:

Trivial vs. Sophisticated Attacks: Although the techniques of attackers are becoming more advanced, it is often the more relatively trivial attacks that the media hypes up. As highlighted, the "hacking" of military drones in Iraq was nothing more than recording and displaying what was arguably accessible information. Still, it is the

technically simple assaults that can generate the most extensive effects, as seen by the DDoS attacks on Dyn. Despite infecting more than 300,000 systems in 150 countries and having dramatic consequences, WannaCry was also, at a technical level, rather rudimentary, in that it only exploited already known vulnerabilities.

On the other hand, it can be seen how there is a growing number of ever more sophisticated attacks. Stuxnet marked the beginning of a new class of cyber attacks, in that a cyber weapon was deployed that led to significant material damage. The same can be seen in the attacks on the power grid in Ukraine, which were long in preparation and affected various kinds of software and systems, including the manipulation of firmware of Industrial Control Systems (ICS). Also, our partial knowledge of the surveillance structures and tools of the NSA and CIA shows they are highly sophisticated, as revealed by the respective leaks.

The trend towards more sophisticated attacks and their development on the timeline leads to the next findings:

Preparation of the Battlefield: A variety of actions in recent years reveals how ever more comprehensively engagement on the cyber battlefield is being prepared. The number as well as the quality of attacks on critical infrastructures is rising, as are infiltration campaigns aimed at installing backdoor access. The preparation of access opportunities also can be seen by different attacks on the supply chain, introducing malevolent hardware that can manipulate whatever software is installed upon it. At the same time, comprehensive cyber espionage activities can be identified, focusing on military systems and developments, as well as blueprints for the development and testing of new cyber weapons being used in the field, e.g., like in the cases of TV5 Monde or the Ukrainian power grid.

Glassy Humanity: The amount and quality of breached data reaches a level that can severely affect many areas of life, but especially people in security-critical tasks and functions. The OPM breaches presented a very severe incident, including data relating to personnel security background checks, while the breaches of the casual dating platforms Ashley Madison and AdultFriendFinder contained very detailed, personal data. Also, medical and personal devices and trackers are collecting more and more data and are often poorly secured, putting them well within the range of hostile online forces.

Further, newly available services like satellite surveillance offered by the company Planet Labs Inc. [95] will make surveillance capabilities previously reserved for the military and states available for almost everybody.

Theoretical vs. Practical Security: Another aspect already visible in the real world and growing in importance is the tension between theoretical and practical security. While having new systems based on mathematically provable security systems like QKD, complex technical implementations open up almost inestimable possibilities for side channel attacks. Being a very powerful and evolving instrument, AI can support cyber security, but at the same time such systems may also produce unpredictable and unwanted results, based on their complexity and "black box" character.

Demonstration of Cyber Power: Finally, some cases of the demonstration of cyber power can already be identified. Eventually, Stuxnet turned out in the demonstration of cyber power, based on the change of the code and attacker behaviour, as well as the too intense public discussions and statements. In part the attack on TV5 Monde and the activities of The Shadow Brokers can be seen as demonstrations of cyber power.

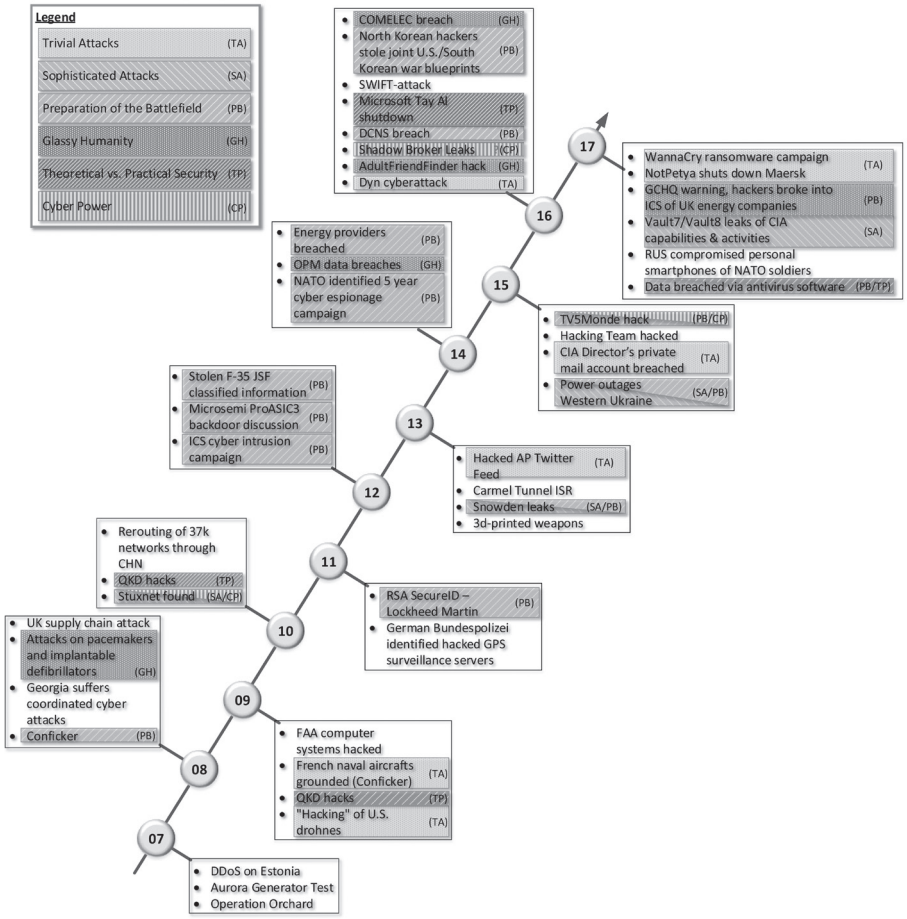
Figure 5 highlights the coherences between cyber security incidents and the derived characteristics.

D. The next 10 Years: A look into the Crystal Ball

Technological evolution is exponential, and IT improvements grow at an even super-exponential rate over long time spans [96]. This is something hard to cope with for human beings in daily life, and often decisions are taken based on a "linear feeling". Having a look at current research programs and activities coupled with various developments and announcements over the last few years provides glimpse of a picture of what we may expect.

The "Defense Innovation Initiative" already mentioned earlier is a good starting point to figure out how tomorrows technical world may look like. By having a look at related programs setup by DARPA, and state-of-the-art research, the following aspects can be identified:

FIGURE 5. COHERENCES OF IMPORTANT CYBER SECURITY INCIDENTS FROM 2007 TO 2017



First, the wide use of practically unlimited storage like 5d Glass discs and DNA storage [97] will challenge encryption security systems. Being able to store everything until one can decrypt it requires stronger encryption methods, and renders traditional concepts of proposed key lengths for certain periods of time as insufficient.

Second, Quantum supremacy will be achieved. While applications like QKD are already available, new techniques for secure communications will become ready for use. More so, universal quantum computers will open new opportunities for simulation, prediction, and security of systems, in the process supplanting and surpassing traditional security concepts. Recent research published by the University of Cambridge [98], IBM, and Intel shows tremendous progress in this area.

Robots and the “Soldier 4.0” concept (technical and bio enhancements to soldiers) will be much more powerful, but to the same degree, much more dependent on IT – ranging from the use of exoskeletons [99] to smart bandages for the faster healing of wounds or selectively erasing memories of trauma from the brain [100]. Of course, technology in \itself is morally inert – there is as much scope for misuse and abuse as there is for beneficent impacts benefiting all mankind.

Self-X technologies will find their way into products used in the real-world. While DARPA’s Cyber Grand Challenge in 2016 demonstrated the potential for self-defending systems to analyse attacks and patch themselves up, the setup was based on tiny, very limited operating systems. Anyway, it shows the future of cyber security, and related programs like “System Security Integrated Through Hardware and Firmware” (SSITH) [101] will raise the bar for attackers.

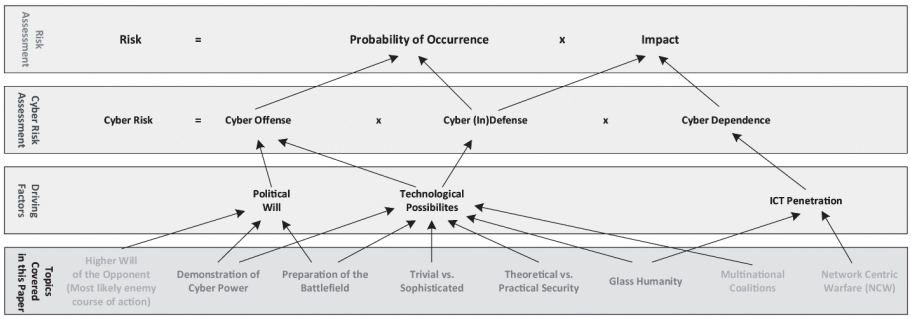
Finally, AI will only increase in power and come to pervade all areas of life, with algorithms achieving ever more superior performance with no human input. Together with more and more powerful and specialized hardware, e.g., self-learning neuromorphic chips that mimic brain functions [102], this will enable completely autonomous systems to operate independently in hostile environments, and much faster than any system reliant on human input in their loop.

Summing up these aspects highlights key elements of tomorrow’s forces: autonomous and collectively mission-executing systems that are produced cheaply and mobile via 3D-printing, that can self-destruct or dissolve in air so the technology will not fall into the hands of the adversary. While this can enable future supremacy on the battlefield even in denied environments (A2AD), the core requirement remains the same – strong cyber security, not only to protect the systems of tomorrow, but also to protect the research, design, and production that led to them.

4. CONCLUSION

Looking back on 10 years of cyber security, the situation seems to be becoming more and more challenging. Cyber is a popular tool for numerous reasons and many players. Upcoming technologies enforce hard and timely decisions, but the opportunities exist for a sustained improvement in cyber security. Figure 6 summarizes the paper and thus visually establishes a relationship between the Sections 2 and 3.

FIGURE 6. MAPPING OF THE IDENTIFIED COHERENCES AND DEDUCTIONS IN CYBERSPACE TO A RISK ASSESSMENT



Basically, risk can be seen as a mathematical product of the factors "probability of occurrence" and "impact of the damage". With respect to cyber, this equation is often extended to a three-factor equation:

Cyber Risk = Cyber Offense x Cyber Defence x Cyber Dependence

Section 2 has outlined how Russia's political will to use cyber weapons has increased. On that point, we have used examples of (i) economic subversion, and (ii) use of cyber attacks in Ukraine and Georgia. Technical developments are manifold and can be subdivided into the categories outlined. As per the actual realization of political will and technical capabilities in conducting cyber warfare, we have seen only the tip of the iceberg and, in the future, we will see cyber powers demonstrated far more often. Many of the attacks thus far could be ascribed to the notion of the "Preparation of the Battlefield". To be able to survive in a cyber war tomorrow, you have to do your homework today, and thus "prepare your opponent". It has to be assumed that countries such as Russia or China have quite different weapons at their disposal. Anyone who believes that these nations find cyber vulnerabilities "by accident" is wrong. Systematic preparation means deliberately finding and exploiting vulnerabilities on your opponent's side, if not indeed actively installing them in the soft- or hardware they may have sourced from you, and not waiting for "luck" to lean in your favour.

For the West, this means we have to think about cyber security more holistically and system-wide, especially in our military forces, and we need more innovative concepts with shorter procurement cycles. The topic of whether or not Western nations need a "critical security industry" is also an issue that needs to be discussed.

For the military, the power of future assertiveness means using NCW and autonomous systems. Fast decision-making requires information superiority and that in turn requires

ICT. Nonetheless, parallel to networking, greater autonomy and decentralization must be given greater consideration. To realize this complex task, sometimes less is more: in order not to end up in the "complexity trap", we should rather stick to the keep-it-simple approach, instead of looking for a vast, single, super solution. This means, in particular, the use of cost-effective systems, which are built to be mission-specific and on time using additive production methods and which are able to fulfil their missions on the basis of AI and swarm behaviour, even under A2AD conditions. Multi-billion dollar, high-value systems intended for use over decades, are only needed to a small extent as part of an overall strategy.

Furthermore, critical systems like weapon or crypto systems need verifiably secure designs. Trusted hardware for selected and highly-critical components as well as verified microkernels like seL4 are ways to realize this.

It is important to realize that the preparation of tomorrow's battlefield is happening now, resulting in backdoors in today's design and production. Therefore, better security along the supply line is required quickly and can be pushed by, for example, the use of Blockchain technologies.

Finally, disruptive technologies can have a huge impact on cyber security. For example, quantum computers will have a huge and immediate impact on cyber security when they are finally realized and deployed on a wholesale, real-world scale. Therefore, preparation is essential, even in the unlikely case that quantum computing does not get beyond the experimental lab stage. Thus, systems must be highly adaptive; for example, algorithms must be exchangeable quickly and comprehensively, but also structures and organizations must be flexible, being able to control and implement the required administrative processes.

REFERENCES

1. Ferbrache, D. (2003). "Network enabled capability: concepts and delivery". *Journal of Defence Science*. Vol. 8, No. 3, pp. 104-107.
2. Cebrowski, A. K., and Garstka, J. J. (1998). "Network-centric warfare: Its origin and future". In *US Naval Institute Proceedings*. Vol. 124 No. 1, pp. 28-35.
3. Alberts, D.S. (2002). "Information age transformation: getting to a 21st century military". *Command and Control Research Program (CCRP)*. Available at: http://www.dodccrp.org/files/Alberts_IAT.pdf [Accessed 10 Apr. 2018].
4. Wilson, C. (2007). "Network centric operations: background and oversight issues for congress". *Congressional Research Service*. Available at: http://www.au.af.mil/au/awc/awcgate/crs/rl32411.pdf [Accessed 10 April 2018] p. 1-55.
5. Lloyd, M. (2004). "Commanding mission groups: a speculative model". *9th International Command and Control Research and Technology Symposium (ICCRTS)*. Available at: http://dodccrp.org/events/9th_ICCRTS/CD/papers/122.pdf [Accessed 10 April 2018].

6. Alberts, D. S., Garstka, J. J., Hayes, R. E., and Signori, D. A. (2001). "Understanding information age warfare". *Command and Control Research Program (CCRP)*. Available at: http://www.dodccrp.org/files/Alberts_UIAW.pdf [Accessed 10 April 2018].
7. Febbraro, A. R., McKee, B., and Riedel, S. L. (2008). "Multinational Military Operations and Intercultural Factors". *NATO Research and Technology Organisation*. Available at: https://pdfs.semanticscholar.org/d67a/090784c6224fb8a3b230b628448e4b67ef0d.pdf [Accessed 10 April 2018].
8. Palin, R. (1995). "Multinational military forces: Problems and prospects". *The Adelphi Papers*. Vol. 35 No. 294.
9. Major, C., and Mölling, C. (2014). "The Framework Nations Concept: Germany's contribution to a capable European defence". *German Institute for International and Security*. Available at: https://www.swp-berlin.org/fileadmin/contents/products/comments/2014C52_mjr_mlg.pdf [Accessed 10 April 2018].
10. Glatz, R., and Zapfe, M. (2017). "Ambitious Framework Nation: Germany in NATO", *German Institute for International and Security* Affairs, Available at: https://www.swp-berlin.org/fileadmin/contents/products/comments/2017C35_glt_zapfe.pdf [Accessed 10 April 2018].
11. Pogodda, S., et al. (2014). "Assessing the impact of EU governmentality in post-conflict countries: pacification or reconciliation?". *European Security*. Vol. 23 No. 3, pp. 227-249.
12. Sanders, K. (2014). "Did Vladimir Putin call the breakup of the USSR 'the greatest geopolitical tragedy of the 20th century?' ". *Politifact.com*. Available at: http://www.politifact.com/punditfact/statements/2014/mar/06/john-bolton/did-vladimir-putin-call-breakup-ussr-greatest-geop/ [Accessed 10 April 2018].
13. Coyle, J. J. (2017). *Russia's Border Wars and Frozen Conflicts*. Cham: Springer.
14. Lesk, M. (2007). "The new front line: Estonia under cyberassault". *IEEE Security & Privacy*. Vol. 5 No. 4, pp. 76-79.
15. Meserve, J. (2007). "Sources: Staged cyber-attack reveals vulnerability in power grid". *CNN*. Available at: http://edition.cnn.com/2007/US/09/26/power.at.risk/ [Accessed 10 April 2018].
16. Makovsky, D. (2012). "The Silent Strike". *New Yorker*. Vol. 17, pp. 34-40.
17. Adee, S. (2008). "The hunt for the kill switch". *IEEE Spectrum*. Vol. 45 No. 5, pp. 34-39.
18. Nahorney, B. (2009). "The Downadup Codex - A comprehensive guide to the threat's mechanics". *Symantec Security Response*. Available at: https://www.symantec.com/connect/sites/default/files/the_downadup_codex_ed1_0.pdf, [Accessed 10 April 2018].
19. Asghari, H., Ciere, C. M., and Van Eeten, M. J. (2015). "Post-mortem of a zombie: Conficker cleanup after six years". *Proceedings of the 24th USENIX Conference on Security Symposium*. Available at: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-asghari.pdf, [Accessed 10 April 2018].
20. Hypponen, M. (2009). "The Conficker Mystery". *BlackHat*. Available at: http://www.blackhat.com/presentations/bh-usa-09/HYPPONEN/BHUSA09-Hypponen-ConfickerMystery-PAPER.pdf [Accessed 10 April 2018].
21. Gorman, S. (2008). "Fraud Ring Funnels Data From Cards to Pakistan". *Wall Street Journal*. Available at: https://www.wsj.com/articles/SB122366999999723871 [Accessed 10 April 2018].
22. Marks, P. (2011). "Air traffic system vulnerable to cyber attack". *New Scientist*. Vol. 211 No. 2829, pp. 22-23.
23. Willsher, K. (2009). "French fighter planes grounded by computer virus". *The Telegraph*. Available at https://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html [Accessed 10 April 2018].
24. Arthur, C. (2009). "SkyGrabber: the $26 software used by insurgents to hack into US drones". *The Guardian*. Available at: https://www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked [Accessed 10 April 2018].
25. Zmijewski, E. (2010). "Accidentally importing censorship". *Renesys Blog*. Available at: https://dyn.com/blog/fouling-the-global-nest/ [Accessed 10 April 2018].
26. Toonk, A. (2010). "Chinese ISP hijacks the Internet". *BGPMON*. Available at: https://bgpmon.net/chinese-isp-hijacked-10-of-the-internet/ [Accessed 10 April 2018].
27. Langner, R. (2013). "To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve". *The Langner Group*. Available at: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf [Accessed 10 April 2018].
28. Hirvonen, T. (2013). "How RSA Was Breached". *PWC*. Available at: https://www.pwc.dk/da/arrangementer/assets/cyber-timohirvonen.pdf [Accessed 10 April 2018].
29. Gary, F. S. (2015). "New Snowden Documents Reveal Chinese Behind F-35 Hack". *The Diplomat*. Available at: https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/ [Accessed 10 April 2018].

30. Majumdar, D. (2015). “America’s F-35 Stealth Fighter vs. China’s New J-31: Who Wins”. *The National Interest*. Available at: http://nationalinterest.org/blog/the-buzz/americasf-35-stealth-fighter-vs-chinas-new-j-31-who-wins-13938 [Accessed 10 April 2018].
31. Skorobogatov, S. and Woods, C. (2012). “Breakthrough silicon scanning discovers backdoor in military chip”. *International Workshop on Cryptographic Hardware and Embedded Systems*. Available at: https://www.cl.cam.ac.uk/~sps32/ches2012-backdoor.pdf [Accessed 10 April 2018].
32. Domas, C. (2017). “Breaking the x86 ISA”. *Blackhat*. Available at: https://www.blackhat.com/docs/us-17/thursday/us-17-Domas-Breaking-The-x86-Instruction-Set-wp.pdf [Accessed 10 April 2018].
33. Peter, F. (2013). “Bogus AP tweet about explosion at the white house wipes billions off US markets”. *The Telegraph*. Available at: https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html [Accessed 10 April 2018].
34. Macaskill, E., and Dance, G. (2013). “NSA files decoded: Edward Snowden’s surveillance revelations explained”. *The Guardian*. Available at https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded [Accessed 10 April 2018].
35. Koerner, B. I. (2017). “Inside the Cyberattack that Shocked the US Government”. *Wired*. Available at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ [Accessed 10 April 2018].
36. Ejinsight (2014). “Russians hack NATO, EU and Ukraine in 5-year espionage”. *Ejinsight.com*. Available at: http://www.ejinsight.com/20141014-Russians-hack-NATO,-EU-and-Ukraine-in-5-year-espionage/ [Accessed 10 April 2018].
37. Symantec Security Response (2014). “Dragonfly: Western Energy Companies Under Sabotage Threat”. *Symantec*. Available at: https://www.symantec.com/connect/blogs/dragonfly-westernenergy-companies-under-sabotage-threat [Accessed 10 April 2018].
38. Corera, G. (2016). “How France’s TV5 Was Almost Destroyed by ‘Russian Hackers’ ”. *BBC News*. Available at http://www.bbc.com/news/technology-37590375 [Accessed 10 April 2018].
39. Lee, R. M., Assante, M. J., and Conway, T. (2016). “Analysis of the cyber attack on the Ukrainian power grid”. E*lectricity Information Sharing and Analysis Centre*. Available at: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf [Accessed 10 April 2018].
40. Symantec Security Response (2016). “SWIFT attackers’ malware linked to more financial attacks”. *Symantec*. Available at: https://www.symantec.com/connect/blogs/swift-attackersmalware-linked-more-financial-attacks [Accessed 10 April 2018].
41. Sang-Hun, C. (2017). “North Korean Hackers Stole US-South Korean Military Plans, Lawmaker Says”. *New York Times*. Available at: https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html [Accessed 10 April 2018].
42. Boyd, C. (2016). “COMELEC breach data released online, fully searchable”. *Malwarebytes*. Available at: https://blog.malwarebytes.com/cybercrime/2016/04/comelec-breach-data-released-online-fully-searchable/ [Accessed 10 April 2018].
43. Evans, G. (2016). “Hacking the sting out of Scorpene: DCNS leak exposes secrets”. *Navaltechnology*. Available at: http://www.naval-technology.com/features/featurehackingthe-sting-out-of-scorpene-dcns-leak-exposes-secrets-5645820/ [Accessed 10 April 2018].
44. Whittaker, Z. (2016). “AdultFriendFinder network hack exposes 412 million accounts”, *Zdnet.com*. Available at: https://www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users/ [Accessed 10 April 2018].
45. Solon, O. (2016). “Hacking group auctions ‘cyber weapons’ stolen from NSA”. *The Guardian*. Available at: https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group [Accessed 10 April 2018].
46. Hilton, S. (2016). “Dyn analysis summary of Friday October 21 attack”. *Dyn*. Available at: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ [Accessed 10 April 2018].
47. Chen, Q., and Bridges, R. A. (2017). “Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware”. *International Conference on Machine Learning and Applications (ICMLA)*. Available at: https://arxiv.org/pdf/1709.08753.pdf [Accessed 10 April 2018].
48. Lawler, R. (2017). “Microsoft patches Windows XP to fight ‘WannaCrypt’ attacks (updated). *Engadget*. Available at: https://www.engadget.com/2017/05/13/microsoft-windowsxp-wannacrypt-nhs-patch/ [Accessed 10 April 2018].
49. Thomson, I. (2017). “NotPetya ransomware attack cost us $300m - shipping giant Maersk”. *Forbes*. Available at: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#7e0f16a34f9a [Accessed 10 April 2018].
50. Lubold, G., and Harris, S. (2017). “Russian Hackers Stole NSA Data on US Cyber Defense”. *Wall Street Journal*. Available at: https://www.wsj.com/articles/russian-hackersstole-nsa-data-on-u-s-cyber-defense-1507222108 [Accessed 10 April 2018].

51. MacAskill, E., Thielman, S., and Oltermann, P. (2017). "WikiLeaks publishes 'biggest ever leak of secret CIA documents' ". *The Guardian*. Available at: https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance [Accessed 10 April 2018].
52. WikiLeaks, (2017). "Vault 7: Projects". *Wikileaks*. Available at: https://wikileaks.org/vault7/ [Accessed 10 April 2018].
53. Denchev, V. S., Boixo, S., Isakov, S. V., Ding, N., Babbush, R., Smelyanskiy, V., Martinis, J., and Neven, H. (2016). "What is the computational value of finite-range tunneling?" *Physical Review X*, Vol. 6 No. 3, p. 031015.
54. Mandrà, S., Zhu, Z., Wang, W., Perdomo-Ortiz, A., and Katzgraber, H. G. (2016). "Strengths and weaknesses of weak-strong cluster problems: A detailed overview of state-of-the-art classical heuristics versus quantum approaches". *Physical Review A*. Vol. 94 No. 2, p. 022337.
55. King, J., Yarkoni, S., Raymond, J., Ozfidan, I., King, A. D., Nevisi, M. M., Hilton, J. P., and McGeoch, C. C. (2017). "Quantum annealing amid local ruggedness and global frustration", arXiv preprint arXiv:1701.04579. Available at: https://arxiv.org/abs/1701.04579 [Accessed 10 April 2018].
56. Moore, S. K. (2017). "IBM Edges Closer to Quantum Supremacy with 50-Qubit Processor". *IEEE Spectrum*. Available at: https://spectrum.ieee.org/tech-talk/computing/hardware/ibm-edges-closer-to-quantum-supremacy-with-50qubit-processor [Accessed 10 April 2018].
57. Nakamoto, S. (2008). "Bitcoin: A peer-to-peer electronic cash system". *Bitcoin.org*. Available at: https://bitcoin.org/bitcoin.pdf [Accessed 10 April 2018].
58. Piscini, E., and Kehoe, L. (2018). "Blockchain & Cyber Security. Let's Discuss". *Deloitte*. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-blockchain-and-cyber-security-lets-discuss.pdf [Accessed 10 April 2018].
59. Shodan (2018). "Shodan.io". Available at: https://www.shodan.io/ [Accessed 10 April 2018].
60. Bodenheim, R., Butts, J., Dunlap, S., and Mullins, B. (2014). "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices". *International Journal of Critical Infrastructure Protection*. Vol. 7 No. 2, pp. 114-123.
61. Gabbatt, A. (2011). "IBM computer Watson wins Jeopardy clash". *The Guardian*. Available at: https://www.theguardian.com/technology/2011/feb/17/ibm-computer-watson-wins-jeopardy [Accessed 10 April 2018].
62. Dehaene, S., Lau, H., and Kouider, S. (2017). "What is consciousness, and could machines have it?". *Science*. Vol. 358 No. 6362, pp. 486-492.
63. Higginbotham, S. (2015). "Who drew this? A computer... or Van Gogh?". *Fortune*. Available at: http://fortune.com/2015/08/31/ai-vangogh/ [Accessed 10 April 2018].
64. Goldhill, O. (2016). "The first pop song ever written by artificial intelligence is pretty good, actually". *Quartz*. Available at: https://qz.com/790523/daddys-car-the-firstsong-ever-written-by-artificial-intelligence-is-actually-pretty-good/ [Accessed 10 April 2018].
65. Hunt, E. (2016). "Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter". *The Guardian*. Available at: https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter . [Accessed 10 April 2018].
66. Staff, R. (2017). "How to Trick Google's AI into Thinking a Turtle is a Gun". *Robotics Business Review*. Available at: http://www.roboticstrends.com/article/how_to_trick_googles_ai_into_thinking_a_turtle_is_a_gun/Artificial_Intelligence [Accessed 10 April 2018].
67. Galeon, D. (2017). "Saudi Arabia Made a Robot a Citizen. Now, She's Calling For Women's Rights". *Futurism*. Available at: https://futurism.com/saudi-arabia-maderobot-citizen-calling-womens-rights/ [Accessed 10 April 2018].
68. Silver, D., Schrittwieser, J., Simonyan, K., Antonoglou, I., Huang, A., Guez, A., Hubert, T., Baker, L., Lai, M., Bolton A., (2017). "Mastering the game of go without human knowledge". *Nature*. Vol. 550 No. 7676, pp. 354-359.
69. Gerasimov, V. (2016). "The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations". *Military Review*. Vol. 96 No. 1, p. 23.
70. Mckew, M. K. (2017). "The Gerasimov Doctrine". *Politico*. Available at: https://www.politico.com/magazine/story/2017/09/05/gerasimovdoctrine-russia-foreign-policy-215538 [Accessed 10 April 2018].
71. Hagel, C. (2014). "The Defense Innovation Initiative". *Department of Defense*. Available at: http://archive.defense.gov/pubs/OSD013411-14.pdf, [Accessed 10 April 2018].
72. Ormandy, T. (2016). "How to Compromise the Enterprise Endpoint". *Google*. Available at: https://googleprojectzero.blogspot.be/2016/06/how-to-compromise-enterprise-endpoint.html [Accessed 10 April 2018].

73. Fox-Brewster, T. (2015). “Netflix is dumping anti-virus, presages death of an industry”. *Forbes*. Available at: https://www.forbes.com/sites/thomasbrewster/2015/08/26/netflix-and-death-of-anti-virus/#7d88b11d18a5 [Accessed 10 April 2018].
74. Lewis, J. A. (2013). “Significant cyber incidents since 2006”. *Center for Strategic and International Studies*. Available at: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity [Accessed 10 April 2018].
75. Landesman, M. (2017). “A Brief History of Malware”. Lifewire. Available at: https://www.lifewire.com/brief-history-of-malware-153616 [Accessed 10 April 2018].
76. Forni, A. A., and van der Meulen, R. (2016). “Gartner Says Worldwide Security Software Market Grew 3.7 Percent in 2015”. *Gartner*. Available at: https://www.gartner.com/newsroom/id/3377618 [Accessed 10 April 2018].
77. Deshpande, S. (2017). “Market Share: Security Software, Worldwide, 2016”. *Gartner*. Available at: https://www.gartner.com/doc/3698417/market-share-securitysoftware-worldwide [Accessed 10 April 2018].
78. Statista - Das Statistik-Portal (2018). “Weltweites Bruttoinlandsprodukt (BIP) in jeweiligen Preisen von 2007 bis 2017 (in Billionen US-Dollar)”. Available at: https://de.statista.com/statistik/daten/studie/159798/umfrage/entwicklung-des-bip-bruttoinlandsprodunkt-weltweit/ [Accessed 10 April 2018].
79. Price Waterhouse Coopers (2018). “The Global State of Information Security Survey 2018”. *PWC*. Available at: https://www.pwc.com/us/en/cybersecurity/information-security-survey.htm [Accessed 10 April 2018].
80. IDG Communications Inc. (2017). “2018 Global State of Information Security Survey”. *IDG*. Available at: https://www.idg.com/tools-for-marketers/2018-global-stateinformation-security-survey/ [Accessed 10 April 2018].
81. Ponemon Institute LLC (2017). “Cost of cyber crime study 2017 insights on the security investments that make a difference”. *Accenture*. Available at: https://www.accenture.com/t20170926T072837Z__w__/usen/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf [Accessed 10 April 2018].
82. Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., and Kijewski, P. (2015). “2020 cybercrime economic costs: No measure no solution”. *10th International Conference on Availability, Reliability and Security*, pp. 701-710.
83. Lewis, J., and Baker, S. (2013). “The economic impact of cybercrime and cyber espionage”. *McAfee*. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf [Accessed 10 April 2018].
84. McAfee (2018). “Economic Impact of Cybercrime - No Slowing Down”. *McAfee*. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf [Accessed 17 April 2018].
85. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, M., and Savage, S. (2013). “Measuring the cost of cybercrime”. In Böhme, Rainer ed., *The Economics of Information Security and Privacy*. Münster: Springer.
86. McAfee, (2014). “Estimating the global cost of cybercrime”. *McAfee*. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf [Accessed 10 April 2018].
87. Verizon (2017). “2017 Data Breach Investigations Report - 10th Edition”. *Verizon*. Available at: https://www.verizonenterprise.com/verizon-insights-lab/dbir/ [Accessed 10 April 2018].
88. The MITRE Corporation (1999). “Common Vulnerabilities and Exposures”. Available at: https://cve.mitre.org/ [Accessed 10 April 2018].
89. OSVDB (2018). “Open Sourced Vulnerability Database”. Available at: https://blog.osvdb.org/ [Accessed 10 April 2018].
90. Risk Based Security (2018). “Vulnerability Statistics”. Available at: https://vulndb.cyberriskanalytics.com/#statistics [Accessed 10 April 2018].
91. Raesene (2015). “Some potential problems extrapolating from data in security”. Available at: https://raesene.github.io/blog/2015/04/17/some-potential-problemsextrapolating-from-data-in-security/ [Accessed 10 April 2018].
92. Jerichoattrition (2015). “A Note on the Verizon DBIR 2015, ‘Incident Counting’, and VDBs”. Available at : https://blog.osvdb.org/2015/04/23/a-note-on-theverizon-dbir-2015-incident-counting-and-vdbs/ [Accessed 10 April 2018].
93. Christey, S., and Martin, B. (2013). “Buying into the bias: Why vulnerability statistics suck”. *BlackHat*. Available at: https://media.blackhat.com/us-13/US-13-Martin-Buying-Into-The-Bias-Why-Vulnerability-Statistics-Suck-WP.pdf [Accessed 10 April 2018].
94. Jerichoattrition (2017). “The Duality of Expertise: Microsoft”. *OVSDB*. Available at: https://blog.osvdb.org/category/vulnerability-statistics/ [Accessed 10 April 2018].

95. Planet Labs Inc. (2018). “Welcome to the insights economy”. Available at: https://www.planet.com [Accessed 10 April 2018].
96. Bui, Q. M., Nagy, B., Farmer J. D., and Trancik, J. E. (2013). “Statistical basis for predicting technological progress”. *PloS One*. Vol. 8 No. 2, p. e52669.
97. Birney, E., Goldman, N., Bertone, P., Chen, S., Dessimoz, C., LeProust, E. M., and Sipos, B. (2013). “Towards practical, high-capacity, low-maintenance information storage in synthesized DNA”. *Nature*. Vol. 494 No. 7435, pp. 77-80.
98. Cambridge Core (2018). “World’s first complete design of a silicon quantum computer chip”. *Cambridge University Press*. Available at: https://www.cambridge.org/core/journals/mrs-bulletin/news/world-s-first-complete-design-of-a-silicon-quantum-computer-chip [Accessed 10 April 2018].
99. Ackerman, E. (2015). “DARPA Tests Battery-Powered Exoskeletons on Real Soldiers”. IEEE Spectrum. Available at: https://spectrum.ieee.org/video/robotics/military-robots/darpa-tests-batterypowered-exoskeletons-on-real-soldiers [Accessed 10 April 2018].
100. Adler, K., Hu, J., Ferguson, L., Farah, C. A., Hastings, M. H., Sossin, W. S., and Schacher, S. (2017). “Selective erasure of distinct forms of long-term synaptic plasticity underlying different forms of memory in the same postsynaptic neuron”. *Current Biology*. Vol. 27 No. 13, pp. 1888-1899.
101. DARPA (2017). “Baking Hack Resistance Directly into Hardware”. *Defence Advanced Research Projects Agency*. Available at: https://www.darpa.mil/news-events/2017-04-10 [Accessed 10 April 2018].
102. Mayberry, M. (2017). “Intel’s New Self-Learning Chip Promises to Accelerate Artificial Intelligence”. *Intel*. Available at: https://newsroom.intel.com/editorials/intels-new-self-learning-chip-promises-accelerate-artificial-intelligence/ [Accessed 10 April 2018].