ETHICS AND ARMED FORCES

CONTROVERSIES IN PEACE ETHICS AND SECURITY POLICY

ISSUE 01/2019

Conflict Zone Cyberspace: Prospects for Security and Peace

SPECIAL

Cyberspace as a Domain of Military Action

zebis

CONFLICT ZONE CYBERSPACE: PROSPECTS FOR SECURITY AND PEACE

SPECIAL: CYBERSPACE AS A DOMAIN OF MILITARY ACTION

EDITORIAL

"Six out of ten internet users worry about cyberwars," reported IT industry association Bitkom in early 2019. It is possible that for many people, the survey conjured up a danger that they had never considered before. But still the story provides a number of points for reflection.

What exactly is a cyberwar, and what do we mean by the term? Could it occur outside of Hollywood sci-fi thrillers? In light of high-profile attacks and the daily activities of criminals and infiltrators in cyberspace, these questions may seem provocative. According to the German Federal Office for Information Security (BSI), there were around 800 million types of malware in circulation in 2018, 25 percent more than in the previous year. But the editorial team at "Ethics and Armed Forces" has nevertheless decided to press the metaphorical reset button.

The introductory article looks at how the threat situation has developed. Despite an increasing tendency to wage inter-state conflicts in cyberspace, using sometimes spectacular DDoS attacks, disruptive software and "weapons" like the famous Stuxnet worm, there is still no consistent understanding of central categories like war and peace in the cybersphere. To contain the risk of escalation, dialog and agreement on key concepts seem all the more important, taking cues from existing disarmament processes and regimes.

Several authors then proceed to examine whether and to what extent it is appropriate to talk about a "war" in cyberspace. It soon becomes clear that this is not an abstract problem of definition. Attempts to pacify the cyber domain via an international law approach have evidently not been very suitable so far. So why has an escalation not happened yet? Why should we nevertheless concern ourselves with the real political risks of its development?

This also raises the question of whether our distinction between internal and external security is still applicable in a "contested space" like cyberspace. How can or should the state regulate the internet realm, to guarantee security? An internet activist and opposition representative in the German Bundestag and a department head from the German interior ministry set out their respective positions.

The increasing digitalization of communication and weapons technology, together with the fear of cyber attacks – for example against critical infrastructures – have led militaries all over the world to prepare for operations in the digital sphere. Germany has established the Cyber and Information Domain command centre (Kommando Cyber- und Informationsraum, KdoCIR) for this purpose. Essays by high-ranking representatives of the Bundeswehr and NATO in this issue's special feature reveal their assessment of the threats, and what their response strategies are.

As always, the editorial team would like to thank everyone who played a part in producing this edition of "Ethics and Armed Forces." Given the rich and varied discussion, we deliberately avoided using the term "cyberwar" in the collective title for this edition. We take the view that you, our readers, have no need for such emotive words to reflect on the many ethical and security implications of waging digitalized conflict.

Dr. Veronika Bock
Director of zebis

MORE RESPONSIBILITY FOR CYBERSPACE – BUT HOW?

Author: ***Götz Neuneck***

Abstract

Götz Neuneck is a leading German expert on arms control policy. He admits that the formulas and mechanisms of international arms control are not directly transferable to militarization tendencies in cyberspace. But he credibly shows that experiences from the evolutionary process of arms control can provide inspiration for confidence-building measures in cyberspace.

Ever greater interconnectedness is not the only factor behind rising vulnerability and a growing threat to international security. Various cybersecurity activities that are supposed to address this phenomenon involve increasingly aggressive operational capabilities, and hold an enormous risk of escalation. The term "cyberwar" is not sufficiently well defined, so every international actor could understand it to mean something different. Enormous uncertainty is the result, since states set different criteria in their military doctrines to determine whether a cyber attack crosses the threshold of war. The United States, for example, has previously referred to North Korean hacking activities as "acts of war". At the same time, according to Neuneck, it seems as though intensifying competition between states is leading to an unstoppable militarization of cyberspace.

So is there any way to consolidate peace in cyberspace? There is no shortage of initiatives – both national and international – trying to achieve just that, and positive examples of a policy of détente in cyberspace already exist. But ultimately, it is yet another case of thinking about responsible action with the end goal in mind. What we need is a concept of the very essence of cyber peace that everyone can agree on, regardless of the notions of cyberwar.

Public and international debates about security and peace in cyberspace and the potential risks of catastrophic cyber conflicts have intensified in recent years. The West has been especially keen to advocate an "open, secure, and peaceful" cyberspace; yet states are preparing for effective cyber defence and have long been actively pursuing intelligence operations in cyberspace. The risk of cyberattacks with fatal consequences is rising because the modern world is becoming increasingly networked and computerized. This trend will accompany the continued push for digitization. Key topics include the Internet of things (IoT) and advanced manufacturing (think 3D printers), as well as the debate around artificial intelligence.

Furthermore, increasingly aggressive forms of cyber operation such as the hack back and cyber offensives are being discussed, prepared, and sometimes even carried out.[1] According to the latest threat analysis by the USA, around 30 states possess offensive cyber capabilities, enabling them to penetrate computers in other states, steal sensitive information, manipulate it, and disrupt automated processes. The USA itself has been a major technological trendsetter in this respect.

Organizations like NATO, the OSCE, and the European Union have also elevated cybersecurity to a new priority level. Confidence building measures are being discussed, as are offensive strategies, deterrence, and arms control proposals.

The German Armed Forces have set up a military branch for cyber defence with a total of 13,500 posts in its newly founded *Kommando Cyber- und Informationsraum* (Cyber and Information Space). On the one hand, its first task is to operate domestically and in countries of deployment as part of active defence so as to draw together and strengthen the use, protection, and operation of the German Amed Forces' IT systems. On the other hand, it also aims to improve and develop the capabilities for reconnaissance and actions in the *Cyber- und Informationsraum.*

But what does this all mean in a world that is increasingly networked and shaped by digital technologies? What global environment is this development taking place in, and what limiting steps can be taken nationally, EU-wide, and internationally? There are no simple answers, given the rate of change in technology and security policy. The mere creation of institutions like the *Cyber-Abwehrzentrum* (Cyber Defence Centre) and a rapid response force by the German Federal Office for Information Security will not be answer enough. If soldiers are to operate in cyberspace, then clear definitions, standards, and rules of behaviour will have to be created to uphold the obligations of international law and prevent a digital arms race. States will also have to lay down appropriate standards and principles to prevent the Internet from becoming even more militarized. So it is becoming increasingly urgent for foreign and peace policymakers to find consistent strategies as a precaution against threats, to distribute resources meaningfully, and to create sound defensive concepts. And at an international level, the EU and Germany will have to position themselves more rigorously in the face of stiffening competition between the USA, China, and Russia.

Fundamentals of conflict in cyberspace

The temporal and spatial limits of today's warfare are blurring. The Internet itself knows no territorial boundaries. Secret operations, hybrid warfare, and propaganda war are common buzz phrases in this context. The inter-agency Cyber Security Strategy for Germany in 2016 pointedly declares: "Internal and external security in cyberspace can no longer be clearly delimited."[2] This insight is neither new nor especially expedient. But it does pose new questions about the responsibility, jurisdiction, and potential efficiency measures of the agencies involved (Federal Ministries of the Interior and Defence and Federal Foreign Office). None of this has an easy answer because many factors in the "brave new cyberworld" remain vague, from the assessment of threats and matters of definition to the effective, competent preparation of appropriate and effective active and passive countermeasures. And the international debate faces numerous obstacles that cannot be circumvented.

Cyberwar is a term often used but almost impossible to define clearly. There is not yet an internationally accepted definition. The current spectrum of cyberattacks is broad and fluid.[3] It ranges from DDoS attacks, data theft, reconnaissance, espionage, and sabotage (Stuxnet), all the way to potentially active warfare.

Military and intelligence services are overcoming technical barriers and are already penetrating the computer systems of other states. Their motives are many: they may be psychological or to prepare for further acts of aggression ("preparing the battlefield"), but they may also aim to weaken an opponent. Such attacks can target not only military facilities, but also industrial ones (oil production, energy supply, financial systems), which means critical civil infrastructure in the broadest sense. Players' motives and capabilities can vary greatly. What is key is that today's software and hardware development leaves many vulnerabilities open, allowing security barriers to be overcome.

The EU and Germany will have to position themselves more rigorously in the face of stiffening competition between the USA, China, and Russia

Cyberattacks may be part of a comprehensive operation and may include military components. Israel, for instance, bombed an incomplete nuclear reactor in Syria after its air defences (i.e. radar and defence missiles) had been electronically disabled. Estonian government, bank, and media websites were blocked in 2007; a Russian youth organization loyal to the Kremlin later declared its responsibility for the attack. Russia probably coordinated cyber operations along with conventional attacks against Georgia in 2008. President Obama announced in 2016 that cyber operations were being used in the offensive against IS. There are other examples. The Stuxnet worm, which was used against Iranian centrifuges, demonstrates the traits of a cyberweapon. It included a carrier with a "payload" whose modular structure allowed it to be used against different targets. The effects of such disruptive malware are hard to gauge. The NotPetya malware was used against the Ukraine by a Russian hacker group, but seems to have accidentally hit the shipping company Maersk, which had to shut down operations briefly. Other examples include the ransomware WannaCry and Bad Rabbit. These activities cause considerable economic and psychological damage, but are not considered direct acts of war.

An increasing number of cyberattacks are being used in today's conflict configurations. Russian hackers probably succeeded in deactivating a high voltage facility near Kiev (Operation Crash Override) in 2016. The 2014 attacks on Sony Pictures were classed as "acts of war" on the part of North Korea by the Obama administration, but there was no military response. Typical backlash to date has included public denouncement, sanctions, and the expulsion of diplomats, but no actual "kinetic" acts of war. This also shows that ultimately, each state alone will decide for itself whether an act of war has taken place.

Ultimately, each state alone will decide for itself whether an act of war has taken place

Progress would be made if the UN Security Council were to develop a clear set of regulations based on the principles of international humanitarian law. Cyberspace has so far been a domain of asymmetrical political warfare, combined with the diplomacy of coercive measures (such as sanctions and embargos). There are also numerous secret Internet operations that might escalate, but have not yet reached a conventional war threshold. But that could change. It should also be stated that cyberweapons can proliferate and be stolen by other states (example: Eternal Blue).

"Militarization of cyberspace" through competition between states?

The US government's worldwide threat assessment places cyberthreats on page one of global dangers, citing Russia, China, North Korea, terrorists, and criminals as players. The US analysis goes on: "Many countries view cyber capabilities as a viable tool for projecting their influence and will continue developing cyber capabilities."[4] Cyber operations against the North Korean missile programme in summer 2017 underscored the USA's aspiration and willingness to take military action in cyberspace – even if their actions did not lead to the desired result in that instance. So far there has been no escalation and the impact has also been limited. But that need not always remain the case. A future war combined with massive cyberattacks is within the realm of possibility.

Strategic documents published by the Trump administration have called the "struggle for power between the USA, Russia, and China" a paradigm for the 21st century, which is why the USA's cyber policy speaks a more aggressive language than it did under Obama. It has been bolstered by interviews with security advisor John Bolton and the language of a vision statement issued by US Cyber Command entitled "Achieve and Maintain Cyberspace Superiority."[5] This calls for "persistent action" to maintain the USA's cyber superiority. Offensive preventative action has thus been declared the norm. This is reflected also against the background of reviving competition in the National Defense Strategy (2018) and National Security Strategy (2017). According to the US military's joint publication on Cyberspace Operations dated June 8, 2018, offensive cyber operations aim to "project power in and through foreign cyberspace."[6] In the new 2018 DoD Cyber Strategy and Cyber Posture Review, one of the central themes is "using cyberspace to amplify military lethality and effectiveness." [7] A study by the Cato Institute concludes from this: "Cyberspace became a domain for soldiers, not just networks of spies."[8]

Russia uses the prefix "information" instead of "cyber," and published a doctrine of

"Information Security" itself in 2016.[9] They are especially concerned about other states destabilizing them through information and psychological influence. Furthermore, their term "information sphere" places much more emphasis on actual information disseminated through the Internet. This means that bans create the possibility of increased censorship in the country. At the same time, Russia wishes to set up its own, easily controllable version of the Internet. Any new cyber doctrine responding to the latest US doctrine is sure to contain more aggressive elements, not least because Russia is strongly suspected by the USA of intervening in the 2016 US presidential elections by means of cyber operations.

China also avoids the term "cyber" and speaks instead of "information threats." It has been carrying out cyberespionage operations for decades, especially against the USA.[10] One element of this is the theft of secret military information, another is the theft of business information (patents and so on). At a meeting between presidents Obama and Xi Jinping in 2015, they agreed on a kind of moratorium, and Chinese attacks did indeed decline. This shows that bilateral agreements can work. But they are unlikely to be able to prevent future digital armament, especially since various other states are preparing themselves for defensive and offensive operations in cyberspace.

Potential peace-consolidating activities for cyberspace – national and international

The international community has been discussing international campaigns, rules, and instruments to prevent a burgeoning digital arms race and attenuate the gradual militarization of the Internet, especially since the Stuxnet incidents in 2010. This poses many new questions. How can we be sure that cyber operations will not lead to real escalation and even acts of war? How can the various players – i.e. states, industry, and civil society – work together to keep the Internet "uniform, secure, and peaceful?" Given the complexity, size, and laws of cyberspace, can principles and rules be set up efficiently and verifiably to prevent catastrophic cyber activities? In contrast to conventional arms control acquis, cyberspace is open to anybody, fast-growing, technologically fast-transforming, and driven primarily by private business interests. So the inclusion of civil society, industry, and business is essential to any future regulation.

In cyberspace, "The best defence is a good defence."[11] The past ten years have seen considerable efforts at various levels to establish and implement shared international rules. The *Tallinn Manuals* (Vol. I and Vol. II) set out rules under international law in the NATO context that address numerous legal questions about the applicability of international law. At a national level, governments are required to protect their own digital structures and make them resilient as part of their precautions against catastrophe and war. This includes raising user awareness, effective early warning systems, and vulnerability analysis, "attribution scanning," and more resilient network structures. Arms export control also has to be involved, since that is the only way to prevent dangerous malware falling into the hands of hostile states.[12]

Furthermore, decision makers have to possess the technological expertise needed to make the right judgements in the event of a crisis. Because cybersecurity is an inter-agen-

The inclusion of civil society, industry, and business is essential to any future regulation of cyberspace

The Author

__Götz Neuneck__ is a physicist and gained a PhD in mathematics at the University of Hamburg to become a Dr. rer. nat (doctor of natural sciences). He worked on strategic issues, military technology, and arms control with the Afheldt working group at the Max Planck Society in Starnberg from 1984 to 1987. He is the deputy director of the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH) and head of the Arms Control and Emerging Technologies research group. He chairs the Physics and Disarmament working group at the German Physical Society (DPG) and belongs to the council of the Pugwash Conferences on Science and World Affairs.

cy task in peacetime and war, there should be more exchange of personnel between federal authorities as well as coordinated training activities which boost "inter-agency resilience." There is also an urgent need for a greater understanding of new technological developments like artificial intelligence. This will necessitate close collaboration between authorities and industry and academics. Standardized end-to-end encryption for communication would be one important step.

More protection and restraint in the event of offensive action are an important prerequisite in maintaining a freely accessible cyberspace. Analyses show that these objectives are dependent upon a state's security policy. Increasingly aggressive competition between the USA, China, and Russia demands a clear position on the part of the European Union. Medium-sized powers like Australia, Germany, and Canada need to develop appropriate cyber rules to establish a "peaceful and stable cybersphere" in the face of states like the USA, Russia, and China. Internationally, important conclusions and concrete proposals for confidence building measures in cyberspace have been drawn up in working groups at a UN level (UN Group of Governmental Experts) and among regional organizations like the OSCE and ASEAN. These include, for example, mutual duties to inform in the event of cyberattacks and when establishing cyber doctrines, and a ban on attacking critical infrastructure.[13] But so far, leading states have lacked the will to pick up on these ideas, implement them credibly, or develop them further in international discourse. Genuine transparency with regard to offensive operative potential, cyber doctrines, and the function of the institutions involved would be a step in the right direction. This would require a shared understanding of key terms like cyberattack and cyberweapon, as well as their harmful dimensions. These things, however, are only vaguely defined, and are therefore open to all kinds of interpretation and future use. States need to develop a shared foundation. A joint glossary sponsored by the UN would be a welcome first step.

The aim of maintaining an "open, peaceful, freely accessible, stable, and secure" cyberspace is in the interests of the world's states

The problem of attribution in cyberspace appears virtually insoluble, yet forensic standards and facilities will have to be developed that are capable of investigating cyber incidents.[14] Things can be learned in this respect from the transparency and verification rules of established arms control (such as the International Atomic Energy Agency, Organisation for the Prohibition of Chemical Weapons, Comprehensive Nuclear-Test-Ban Treaty Organization).

Soldiers need to be trained so that they are able to apply the principles of international humanitarian law, even in cyberspace conflicts (especially proportionality, the need to discriminate, and military necessity). Joint exercises between friendly states could help to gather experience and surmount crises together.

Companies like Microsoft ("Digital Geneva Convention") and Siemens ("Charter of Trust") have drawn up certain proposals and principles aimed at positively guiding the behaviour of companies and individual users towards a "stable and peaceful" Internet. The non-profit organization Access Now campaigns worldwide for the protection of users' digital rights, and offers help whenever users are attacked or spied on. The "Paris Call for Trust and Security in Cyberspace" initiated by President Macron has found many supporters, and advocates adherence to fundamental principles in this sphere.[15] This will certainly help to build awareness and responsibility in important user groups, but is hardly likely to reach difficult state players in the intelligence services and military organizations of some countries.

In the medium term, transparency and arms control regulations will be needed if demonstrable acts of war using disruptive cyber tools become a possibility. It seems unlikely that today's arms control architecture could be translated straight into a ban on cyberweapons, since cyberspace is extremely difficult to control, cyberweapons are intangible, and they have different harmful outcomes.[16] And yet the aim of maintaining an "open, peaceful, freely accessible, stable, and secure" cyberspace is in the interests of the world's states. Much can be learned from decades of development in treaty-bound arms control regulations when it comes to limiting dangerous attack vectors, avoiding catastrophic harmful effects, and preventing uncontrolled escalation.

In the longer term, there is also the question of what we understand by the lasting cyber peace which many players are repeatedly calling for. Scott J. Shackelford writes about this: "Cyber peace is not the absence of attacks or exploitations, an idea that could be called negative cyber peace. Rather, it is a network of multilevel regimes working together to promote global, just, and sustainable cybersecurity by clarifying norms for companies and countries alike to help reduce the risk of conflict, crime, and espionage in cyberspace to levels comparable to other business and national security risks."[17] Interestingly, this helpful definition lacks the term war. There is still much work to do.

My thanks to Jantje Silomon, Oxford and Hamburg, for her in-depth comments and sources.

[1] See for example the US Congress Cyber Defense Certainty Act, tabled by Tom Graves in March with an amendment. https://www.congress.gov/bill/115th-congress/house-bill/4036 (accessed April 26, 2019).

[2] Federal Ministry of the Interior (2016): *Cyber-Sicherheitsstrategie für Deutschland 2016* [Cyber Security Strategy for Germany in 2016]. Berlin, p. 5. https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (accessed April 26, 2019).

[3] According to an analysis by the Cato Institute, there were 272 documented cyber operations between 2000 and 2016, of which 32.7% were disruptive, 54.4% espionage, and 12.89% subversive. See Maness, Ryan C./Valeriano, Brandon/Jensen, Benjamin (2017): "The Dyadic Cyber Incident and Dispute Dataset Version 1.1."

[4] Coats, Daniel R. (2017): "Worldwide Threat Assessment of the US Intelligence Community." Senate Select Committee on Intelligence, May 11, 2017, p. 1. https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf (accessed April 26, 2019).

[5] U.S. Cyber Command (2018): "Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command." April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010 (accessed April 26, 2019).

[6] U.S. Joint Chiefs of Staff (2018): "Cyberspace Operations." Joint Publication 3-12, June 8, 2018, p. II-5. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (accessed April 26, 2019).

[7] U.S. Department of Defense (2018): "Fact Sheet: 2018 DoD Cyber Strategy and Cyber Posture Review. Sharpening our Competitive Edge in Cyberspace." https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pdf (accessed April 26, 2019).

[8] Valeriano, Brandon/Jensen, Benjamin (2019): "The Myth of the Cyber Offense. The Case for Restraint." Cato Institute, Policy Analysis No. 862, January 15, 2019, p. 4. https://object.cato.org/sites/cato.org/files/pubs/pdf/pa862.pdf (accessed April 26, 2019).

[9] "Information Security Doctrine of the Russian Federation." https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf (accessed April 26, 2019).

[10] Inkster, Nigel (2013): "Chinese Intelligence in the Cyber Age." In: *Survival* 55 (1), February–March 2013, pp. 45–65.

[11] Valeriano, Brandon/Jensen, Benjamin (2019): "The Myth of the Cyber Offense. The Case for Restraint." Cato Institute, Policy Analysis No. 862, January 15, 2019, p. 10. https://object.cato.org/sites/cato.org/files/pubs/pdf/pa862.pdf (accessed April 26, 2019).

[12] Granick, Jennifer (2014): "Changes to Export Control Arrangement Apply to Computer Exploits and More." The Center for Internet and Society, January 15, 2014. https://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more (accessed April 26, 2019).

[13] See Neuneck, Götz (2014): "Cyberwarfare: Hype or New Threat?" In: *Ethics and Armed Forces* 2014/2, pp. 26–31. http://www.ethikundmilitaer.de/en/full-issues/20142-cyberwar/neuneck-cyberwarfare-hype-or-new-threat/ and the entire edition themed on cyberwar (accessed April 26, 2019).

[14] The NGO ICT4Peace has proposed a network organization for stateless attribution. See: "Trust and Attribution in Cyberspace: An ICT4Peace proposal for an independent network of organisations engaging in attribution peer-review." December 6, 2018. https://ict4peace.org/activities/trust-and-attribution-in-cyberspace-an-ict4peace-proposal-for-an-independent-network-of-organisations-engaging-in-attribution-peer-review/ (accessed April 26, 2019).

[15] https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in (accessed April 26, 2019).

[16] See for example Tikk, Eneken (2017): "Cyber: Arms Control without Arms?" In: Koivula, Tommi/Simonen, Katariina (ed.): *Arms Control in Europe: Regimes, Trends and Threats.* Helsinki, pp. 151–187.

[17] Shackelford, Scott J. (2014): *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace.* Cambridge, p. 365.

"CYBERWAR": PAST AND PRESENT OF A CONTESTED TERM

Author: ***Philipp von Wussow***

Abstract

Philipp von Wussow takes a closer look at the shifting concept of "cyberwar." He identifies two extreme positions in the current debate. Both bear little relationship to the actual technical potential of cyber attacks, and have more in common with fears from the Cold War era. On the one hand, some believe that humanity is threatened by catastrophic cyberwar scenarios, or even total annihilation ("cybergeddon"). For those in the opposite camp, it is wrong to talk about "cyberwar," since this only encourages the military and intelligence services to take control of the internet, and raises the risk of escalation.

At core, according to the author, the real issue is that that the ubiquity of cyber crime and cyber espionage makes the "permanent exceptional state becomes the new normal state." Thus the conventional dichotomy of war and peace no longer fits. Characterized by struggles for hegemony and latent danger, this state of uncertain state" could best be compared to a Hobbesian state of nature – the war of all against all.

And yet, von Wussow continues, it is foreseeable that this anarchic status quo (corresponding to the Hobbesian model) will be contained by various processes, because in the long term this is in the interest of the major players. But any "top-down" formation of norms, for example via instruments of international law, seems less suited to this purpose than the development of best practices that emerge from the cyber world itself. Case law on liability issues and the establishment of industrial standards will also play a significant role. In the author's view, the sheer number of authorities involved in these processes and the prevailing division of tasks between state and private sector refutes the idea of a "militarization" of cyberspace. Equally, given the potential threat posed by a possible cyber attack, the military should not be denied all powers of cyber defense.

Despite all the technological capabilities, a global, catastrophic cyberwar has not happened yet and is not likely to happen in the foreseeable future. Yet, at the same time, cyberwar is in our midst, since internet-based attacks have become virtually an everyday occurrence. How do these two observations fit together, and how does this paradoxical discovery impact on our notions of war and peace? Finally, is "cyberwar" really the appropriate term to use in this situation? And, furthermore, is the military really suited to guaranteeing cyber security in the situation we find ourselves in?

To determine whether "cyberwar" is an accurate term, it would seem advisable first of all to review the history of the term and the respective threat scenarios. This gives us a better understanding of the fragile strategic situation where, despite the omnipresence of cyber attacks, there is no realistic prospect of major cyberwars. What is it that ensures cyberwar is largely limited to everyday cyber attacks? In the current literature, this limitation is being discussed with regard to the emergence of norms – a broad term that can encompass such different aspects as diplomacy, strategic deterrence, ethical limitations and liability issues.

Two extreme positions

The term "cyberwar" was coined in 1993 by security experts John Arquilla and David Ronfeldt. It described the "future of warfare" in the context of an IT-driven transformation of military systems, and the resulting reorganization of warfare.[1] Arquilla and Ronfeldt were thinking mainly of terror attacks by non-state actors, although they also sought to describe the increasing integration of cyber components into military defense systems. The cyber terrorism scenario is typical of an initial phase of awareness that extended into the early 2000s. It yielded to a second phase where the focus shifted mainly onto states. Public awareness reached a peak in 2009/10, when the first state or state-sponsored cyber attacks had demonstrated the dangers and capabilities of the new technology on a large scale for the first time. For a moment, in the collective imagination of Western populations, "cyberwars" appeared to be the next great threat to mankind. This entailed a revival of Cold War era fears of an impending nuclear annihilation of mankind.

Even though the problem has changed in many respects since then, plenty of ideas and terms from the 1990s are still circulating in the debate on cyberwars. But the fact that failed ideas live on – such as the cyber terrorism scenario, where ideologically motivated hackers cause a real-world disaster from their PCs – is merely a sign of a more fundamental strategic uncertainty. The ideological field broadly divides into two camps. The most extreme elements set the tone in each camp, while the many moderate voices are caught up in the polemic against the extreme positions. According to these positions, either there is a threat of major cyber catastrophes of hitherto unimagined proportions, or the cyberwar threat is just a pretext, and the real threat is a militarization of the internet.

The prospect of global "cyberwars" has opened up new threat scenarios that take the place of earlier scenarios of nuclear annihilation. According to such descriptions, civilization threatens to be wiped out by the destruction of critical infrastructures. Cyberwars have therefore reactivated latent fears of an impending nuclear war – the real possibility that mankind will be annihilated – and occupied the position left vacant in the collective imagination. The corresponding keywords are "cyber 9/11", "cyber Pearl Harbor", "cyber armageddon" (or "cybergeddon"), occasionally also "cyber Holocaust."

In this scenario, terror groups, hacker groups, script kiddies and other states fight against Western states. They do so primarily by crippling critical infrastructures on a large scale.

Critical infrastructures are everything that keeps modern civilization running, particularly energy and water supplies, transportation, health, banking and agriculture. Usually these areas are not under state control, but nevertheless they are of vital interest to the state, and their potential loss represents a threat to sovereignty. Power stations, hospitals and transport routes (including ports and airports), but also communication networks, must be protected, for any destruction or disruption of theseinfrastructures would paralyze civilian life and potentially produce many victims. Increasing digitalization has made these facilities vulnerable to cyber attacks. Some fear that hackers could open dams and cause a wave of flooding; or they could make trains derail (preferably goods trains carrying toxic chemicals); or take control of self-driving cars and repurpose them as weapons. By attacking power stations, they could cause power outages in urban centers (or even across whole countries). These attacks would be accompanied by a temporary disruption of communication networks. Perhaps the most extreme – and still futuristic-sounding – idea is that the "smart city" of the near future could be taken over by hackers, making life hell on earth for its inhabitants.

The ideological field broadly divides into two camps. The most extreme elements set the tone in each camp, while the many moderate voices are caught up in the polemic against the extreme positions

Despite the possibility in principle, so far no such large-scale cyber attacks on critical infrastructures have occurred. Known ransomware attacks on hospitals (such as the attack on the Lukas-Krankenhaus in Neuss and two other hospitals in North Rhine-Westphalia in February 2016) and municipal authorities did not achieve anything like the imagined extent of civilian damage or level of strategic threat. Great dystopias envisioning the destruction of critical infrastructures by hackers have remained the stuff of cyberwar folklore. The key point here is that such large-scale attacks on critical infrastructures have no strategic benefit for state actors, whereas non-state actors – who could be tempted into such a course of action even without a strategic reason – are not capable of carrying them out. The operational requirements have become too high, and such attacks lack strategic value.[2] They would only become strategically plausible in the context of a greater war strategy, but this would also limit their scope. Temporarily disabling infrastructures in war – e.g. to cut off the enemy's electricity supply – would probably rather result in a decrease in physical destruction. Indeed this has been one of the cyberwar scenarios from the beginning.

The media reaction to these catastrophic scenarios also tested many of the arguments that are still put forward today, in ever new combinations, against the term "cyberwar." Critics not only take exception to sensationalist word combinations like cyber 9/11, cyber armageddon, or cyber Pearl Harbor, they also essentially dispute that such a thing as cyberwar exists. They believe that the term "cyberwar" is merely an ideological construct, employed by states to gain new enemies and new powers. China and Russia – the two big state players in the fight against the Western order – only commit cyber espionage or cyber crime, they argue, but are not interested in a cyberwar. In 2012, the political scientist Thomas Rid summed up this point of view by stating that instead of a cyberwar, there were only different versions of subversion, espionage and sabotage.[3]

One key figure in this debate was the journalist Seymour Hersh. In an influential 2010 article, he described "cyberwar" as a struggle between civilian and military/intelligence use and control of the internet, in which the military and state security services would increasingly attempt to take over the internet. According to Hersh, the great fears are due to a confusion between cyberwar and cyber espionage. This only benefits the defense industry, whereas it is demoralizing for data protectionists. In his view, talk of cyberwar only creates a justification for government agencies to spy on their citizens. Instead, like many before and after him, Hersh calls for a greater use of encryption technologies, including state-mandated encryption: "The government would compel both corporations and individuals to install the most up-to-date protection tools."[4] Only the military and security services would prevent such a solution, as it would limit their ability to intercept signals.

At core, the apodictic rejection of the cyberwar concept serves to stating that cyber attacks should not serve as a casus belli

U.S. cyber security expert Amit Yoran adopts a confusing position. On the one hand, he asserts "serious implications [...] in calling the cybersecurity crisis a cyberwar. A warfare connotation or cyberwar label provides for a natural inclination to place greater emphasis on the role of the military and intelligence community." On the other hand, he too believes that: "Ultimately, it doesn't matter how you define cyberwar or whether you believe we are currently at a state of cyberwar or not."[5] There is no need to point out that the two positions ("serious implications"/"it doesn't matter") are completely incompatible. But the contradiction reflects a widespread uncertainty about the relationship between language and things. Yoran regards the expression firstly as a "label" and thus seems to suggest that the linguistic designation alone could be capable of constituting an act of war – as though war were brought into being only in the act of naming, instead of the naming being a response to a war-like situation. In the second quotation, on the other hand, common sense returns: what matters in reality is not so much the precise term, but primarily the "action." At last, Yoran attempts to bring together the two contrasting aspects with an utterly trivial rhetorical formula: "While definitions matter, the time for action is now."[6]

At core, the apodictic rejection of the cyberwar concept serves to stating that cyber attacks should not serve as a casus belli. There are fears that the United States (or other Western countries) could use a cyber attack as justification for entering into a "real" war. It is highly characteristic of the quality of this debate that the mere fear appears to prohibit from the outset any in-depth investigation of the question of whether cyberwar exists, and what form possible cyberwars of the future could take. Yet the concern is far less justified than it first appears. Western military doctrines certainly allow for a response to a cyber attack using conventional military means. But this forms part of the strategic deterrent, particularly against states that are barely vulnerable to cyber counter-attacks. (The North Korean internet comprises just 28 websites.) Yet no state would go to war over espionage or ransomware attacks.

War and peace

At this point, it is useful to make a few conceptual distinctions. Typically, the term "cyberwar" is used to describe three very different things:

1. According to one concept, it is a war between two sovereign states, conducted mainly using cyber means, i.e. it is largely non-kinetic. In contrast to cyber crime and cyber espionage, cyberwar in this sense has not happened to date, nor is there

any sign that it will happen in the near future. One commonly accepted exception is Stuxnet, the presumed American-Israeli attack on nuclear facilities in Natanz (Iran). It is disputed, however, whether this attack can reasonably be called an act of war.

2. The term cyberwar is also used when limited cyber attacks are carried out in preparation for a so-called kinetic war. Cyber technology is now deeply integrated into many weapons systems. Wars of the future will therefore to a large extent *also* contain cyber elements. But it seems that such an integration of cyber elements into war will ultimately make the notion of cyberwar obsolete. In the meantime, this application of cyber technology has tended to reduce kinetic destruction and hence to contain war – a factor that formed part of cyberwar scenarios from the beginning and remains a decisive argument against the great cyber dystopias.[7]

3. Another view sees the omnipresence of cyber crime and cyber espionage (which *can* develop into a full-scale war at any time, but is not actually developing into such a war) as a new kind of war, in which the permanent state of exception becomes the new normal state. This is not war in the sense codified in international law, but rather a kind of pre-legal state of war akin to Hobbes' state of nature, the fight of all against all.[8] It is particularly in this sense that cyberwar challenges our notions of war and peace.

This cyber natural state forms a gray area between cyber crime, cyber espionage and cyberwar in the narrower sense. For now, we will have to live with the lack of conceptual clarity, and accept that "cyberwar" can refer both to something different than cyber crime and cyber espionage, and to the sum of all three. Broadly speaking, cyber crime forms the technological avant garde, while cyber espionage is the area where states and state-sponsored organizations are developing their cyber capacities. Cyber attacks in the narrow sense are characterized in that they bring the capacities of cyber crime and cyber espionage to a new level of precision and effectiveness. Such attacks are exceptionally rare (Stuxnet is perhaps the only example that meets all criteria), extremely expensive to prepare, limited in their scope, and unreproducible. At the same time, they are possible in principle and constitute an ongoing strategic threat.

In the vast majority of cases, cyberwar takes place in that gray area between cyber crime and cyber espionage. To a large extent, this appears to be the new kind of war in the 21st century. The real point here is that it then becomes almost impossible to distinguish between war and peace. George Lucas describes this kind of war as "ongoing, unrestricted warfare – warfare without rules, 'war of all against all' [...]. The danger is that such warfare not only blurs the lines between war and 'mere' criminal activities, but that such a state of war also becomes increasingly difficult to distinguish from peace."[9]

One view sees the omnipresence of cyber crime and cyber espionage as a new kind of war, in which the permanent state of exception becomes the new normal state

If it is true that this kind of cyberwar is the new kind of war in the 21st century, then the definition of cyberwar moves away from its dependence on Clausewitz's concept of war: "War is [...] an act of force to compel the enemy to do our will."[10] In the cyberwar debate, this concept is preferred particularly by those who base their arguments on the "just war" and the criteria of the *casus belli*. What is actually new about cyberwar, however, is the general uncertainty as to whether and to what extent it is a war at all – the uncertain state between war and peace. The strategic threat posed by cyberwars creates a permanent state of war in peacetime.

Accordingly, we should not so much follow Clausewitz, and instead return to Hobbes and the idea of a war of all against all, a state in which man, "in the care of future time, hath his heart all day long, gnawed on by feare of death, poverty, or other calamity; and has no repose, no pause of his anxiety, but in sleep."[11] This state, which for Hobbes was characterized by the absence of a strong king, has its modern-day equivalent in the absence of a unipolar world power, and struggles for hegemony in a multipolar world. Cyberwar is the means of choice for aspiring great powers. It is a way to challenge the still strong United States within this system of coordinates, and gain technological, informational, economic or ideological advantages.

Norms for cyber warfare

For Hobbes, the idea of the war of all against all was supposed to motivate the *renunciation* of the natural state and the establishment of civilization. There are many indications that the 21st century is facing a similar process with regard to the cyberwar of all against all. But how can this cyber natural state be contained? Is it a matter for international law, in which the classical norms of (analog) war can be applied to cyberspace?

The U.S. and China stand to gain little, but lose a lot, in a cyberwar

The original enthusiasm for international law, as was still apparent in the so-called Tallinn Manual (2013/17), is increasingly giving way to a more complex understanding of the processes in which norms for cyberwar are only just forming.

Individual potential "strong" norms – such as restricting attacks to narrow military targets, banning cyber first strikes, or the obligation to prevent non-state attacks from within one's own territory – have not yet found much acceptance, especially among the big players. But these big players also have little interest in a major cyberwar. In part, and paradoxically, this is rooted in the principle of mutually assured destruction, comparable to the prospect of mutual nuclear annihilation during the Cold War. In particular, deterrence explains why there has been no cyberwar to date between the U.S. and China – two of the three biggest players – and why any such cyberwar has little strategic value. China could at any time cross the line from cyber espionage to cyber warfare against the United States, or at least that is what a number of major hacks suggest. And the United States, for its part, could attack China, especially where it could exploit security vulnerabilities created by Chinese product piracy. Both stand to gain little, but lose a lot, in a cyberwar.

Hence there is a common interest in not allowing a major cyberwar to happen despite all the various different goals. It would seem that this interest has also driven the recent rise of cyber diplomacy. Looking at the relevant initiatives, especially by the European Union, for the time being the main concern is with dialog and confidence building between the cyber powers. Ideally, diplomatic dialog leads to agreements below the threshold of law, which then acquire the force of law over time.

Moreover, norms for cyberwar are also formed in interaction with the private sector, for example in the fast-growing market for cyber insurance. In the near future, landmark court decisions on liability issues will give a new impetus to the emergence of norms. The scope will extend considerably beyond the topic of self-driving cars, which has achieved such high media visibility. For the time being, then, law will primarily emerge from court rulings on liability issues associated with damage caused by cyber attacks. For example, the insurance issues around Not Petya – a suspected Russian cyber attack against the Ukraine, in which a ransomware attack (Petya) was used as cover – revolve around the question of whether this was an attack by the Russian state, and therefore an act of war. The Mondelez group filed a complaint against the Zurich Insurance Group, which had refused to pay out on the basis of a war exclusion clause. Now the issue will be decided by an American court. This case is highly significant for the emergence of norms for cyber warfare and will undoubtedly also have an impact on the formation of norms for cyber attacks between states. But the way to deal with threats will also greatly change due to the establishment of good practices and industry standards. Cyber ethics should primarily reflect on and critically engage in these processes, instead of seeking to provide cyber practice with a normative concept that plays no role in the actual norming processes.

The multipolar world of cyber security

If we look at such examples of norming processes and the authorities involved in them, then it also becomes apparent that the feared "militarization" of cyberspace has not taken place. The military is one of many players in the national cyber defense field, but it has not brought cyberspace "under control". Particularly in Germany, with its federal structures, the German armed forces *(Bundeswehr)* share their tasks with a State

Office of Criminal Investigation *(Landeskriminalamt)* in each of the Länder, the German Federal Intelligence Service *(Bundesnachrichtendienst,* BND), the German Federal Office for Information Security *(Bundesamt für Sicherheit in der Informationstechnik,* BSI) and various ministries. Internationally, national cyber defense is integrated into NATO and the EU. Moreover, limited but highly effective alliances emerge time and again, including Five Eyes (Australia, Canada, New Zealand, United Kingdom, United States) together with their various extensions, some of which include Germany (Eight Eyes, Nine Eyes, Fourteen Eyes). At the same time, the business sector, private IT security firms and cyber insurance companies have an increasingly large stake in cyber security.

In this multipolar world of competences and responsibilities, the military component is an important element. It will be most significant if an attack is of a military nature – meaning not only the objectives, but also the type of attack, i.e. the degree of complexity and strategic depth. In the realms of everyday cyber crime, state bodies perform defense tasks only to a limited extent. They largely play a coordinating role, and may also exert an influence on the cyber security of businesses, infrastructures and private users by formulating minimum technical standards – for example in the context of public contracting – or setting legal frameworks.

Thus we should not place too high expectations on military cyber defense. In the normal case the military's actual cyber defense tasks are in an area that cannot be served by other players. In the case of emergency, since the armed forces have greater capabilities and powers, they can adopt a stronger coordinating role. Discussions about the necessary capacities and powers of the *Bundeswehr* cyber command have largely focused on the question of whether, in the event of an attack, it can remain true to its defensive mandate, or whether it may also be allowed to "hack back", e.g. to switch off an attacker's server. It could also disconnect parts of Germany's infrastructure, to temporarily prevent access by military attackers. While blanket military control of the internet would hardly be desirable, there is little reason to forego the relative protection of military cyber commands.

[1] Arquilla, John / Ronfeldt, David (1993): "Cyberwar is Coming!" In: *Comparative Strategy,* 12 (1) pp. 141–165, reprinted in: Arquilla, John/Ronfeldt, David (eds.) (1997): *In Athena's Camp. Preparing for Conflict in the Information Age.* Santa Monica, pp. 23–60.

[2] Lewis, James Andrew (2018): "Rethinking Cybersecurity. Strategy, Mass Effect, and States." https://www.csis.org/analysis/rethinking-cybersecurity (accessed April 25, 2019).

[3] Rid, Thomas (2012): "Cyber War Will Not Take Place." In: *The Journal of Strategic Studies,* 35 (1), pp. 532, p. 6; cf. by the same author (2013): *Cyber War Will Not Take Place.* London.

[4] Hersh, Seymour M. (2010): "The Online Threat: Should We Be Worried About a Cyber War?" In: *The New Yorker,* November 1, 2010.

[5] Yoran, Amit (2010): "Cyberwar or Not Cyberwar? And Why That Is the Question." In: *Forbes,* March 25, 2010. http://www.forbes.com/sites/firewall/2010/03/25/cyberwar-or-not-cyberwar-and-why-that-is-the-question/ (accessed April 25, 2019).

[6] Ibid.

[7] Arquilla, John (2012): "Cyberwar Is Already Upon Us. But Can It Be Controlled?" In: *Foreign Policy,* February 27, 2012. http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/ (accessed January 15, 2019).

[8] For Hobbes, the threshold for a state of war lies before the imminent danger of an escalation: "For WARRE, consisteth not in Battell onely, the act of fighting; but in a tract of time, wherein the Will to contend by Battell is sufficiently known: and therefore the the notion of Time, is to be considered in Warre; as it is in the nature of Weather. For as the nature of Foule weather, lyeth not in a showre of rain; but in an inclination thereto of many dayes together: So the nature of War consisteth not in actual fighting; but in the known disposition thereto, during all the time there is no assurance to the contrary. All other time is PEACE." Hobbes, Thomas (1996). *Leviathan.* R. Tuck (ed.) Cambridge, pp. 88–89.

[9] Lucas, George (2017): *Ethics and Cyber Warfare. The Quest for Responsible Security in the Age of Digital Warfare.* New York, p. 9.

[10] Clausewitz, Carl von (1973): *Vom Kriege.* 18th edition. Bonn, pp. 191 ff. (translated from German).

[11] Hobbes, Thomas (1996): *Leviathan.* R. Tuck (ed.) Cambridge, p. 106.

The Author

Philipp von Wussow studied philosophy, German literature, and information science at Heinrich Heine University Düsseldorf. In 2004/5, he was a visiting fellow at the Hebrew University of Jerusalem. He received his PhD in 2006 with a dissertation on Theodor W. Adorno. He held positions at Leipzig University from 2007 to 2013, and at Goethe University Frankfurt am Main from 2014 to 2016. In 2016/17 he was a visiting research fellow at the University of Pennsylvania, Philadelphia. He gained his habilitation at the Goethe University in 2017. In 2018, Philipp von Wussow became principal investigator of a project on cyber ethics at the Institute for Theology and Peace (ithf) in Hamburg.

PROSPECTS FOR PEACE IN THE CYBER DOMAIN

Author: *George R. Lucas*

Crying "Peace! Peace!" when there is no peace in the cyber domain

Abstract

In his philosophical essay, George R. Lucas examines a fundamental ethical dilemma in Hobbes's original, otherwise strictly amoral account of the State of Nature: How should man bring about what appears to be a morally required transition to a more stable political arrangement, comprising a rule of law under which the interests of the various inhabitants in life, property and security would be more readily guaranteed? Hobbes described opposition to this morally requisite transition as arising from "universal diffidence," the mutual mistrust between individuals, coupled with the misguided belief of each in his or her own superiority. His, the author argues, is thus a perfect moral framework from which to analyze prospects for attaining peace in the cyber domain.

With his framework in place, it can be quickly noted that the chief moral questions pertain to whether one may already discern a gradual voluntary recognition and acceptance of general norms of responsible individual and state behavior within the cyber domain, arising from experience and consequent enlightened self-interest, or whether the interests of the responsible majority must eventually compel some sort of transition from the state of nature by forcibly overriding the wishes of presumably irresponsible or malevolent outliers in the interests of the general welfare. Lucas leaves no doubt that we should approach the norm-building process descriptively, and put up with the relative legal freedom of cyberspace, rather than deciding on the morally unacceptable second solution.

When we are not engrossed by (for example) the latest technologies available through the Internet of Things, it seems that our reflections concerning the cyber realm turn instead to the endless conflicts and prospects for "virtual war" in that domain. But what of the prospects for peace? To what extent is peace, rather than war, a desirable state in this domain? Even more to the point: how willing are the various agents who populate this domain to invest in efforts aimed at achieving the goal of peace, rather than persisting in their present condition of seemingly endless and intractable strife?

At first, nothing could seem less promising than attempting to discuss "peace" in this context. Even apart from the moral conundrums of outright warfare, the cyber domain generally is often described as a "lawless frontier" or a "state of nature," in which everyone seems capable in principle of doing whatever they wish to whomever they please without fear of attribution, retribution, or accountability. When it comes to human behavior, and the treatment of one another, human behavior within the cyber domain might aptly be characterized, as above, as a "war of all against all."

Upon further reflection, however, that grim generalization of our actual condition is no more or less true than Hobbes's own original characterization of human beings themselves in a hypothetical state of nature. If we stop to consider it, the vast majority of actors in the cyber domain are relatively benign: they mind their own business, pursue their own ends, do not engage in deliberate mischief, let alone harm, do not wish their fellow citizens ill, and generally seek only to pursue the myriad benefits afforded by the cyber realm: access to information, goods and services, convenient financial transactions and data processing, and control over their array of devices from cell phones to door locks, refrigerators and toasters, voice assistants like Alexa and Echo, and even swimming pools.

Beyond this, there are some "natural virtues" and commonly-shared definitions of the Good in the cyber domain: anonymity, freedom, and choice, for example, and a notable absence of external constraints, restrictions and regulations. These are things that cyber activists, in particular, like to champion, and seem determined to preserve against any encroachments upon them in the name of the "rule of law." In essence, we might characterize the cyber domain as colonized by libertarians and anarchists who, if they had their way, would continue to dwell in peace and pursue their private and collective interests without interference.

Like all relatively ungoverned frontiers, however, this natural tranquility is easily shattered by the malevolent behavior of even a few bad actors. And there are more than a few "bad actors" in the cyber domain. As a forthcoming book by Australian cyber security experts Seumas Miller and Terry Bossomaier portrays the matter,[1] the principle form of malevolent cyber activity is criminal in nature: theft, extortion, blackmail, vandalism, slander and disinformation (in the form of trolling and cyber bullying), and even prospects for homicide.

Philipp von Wussow accordingly writes in this issue that the "warfare" in question within the cyber domain is that described by Thomas Hobbes, rather than the more recent and conventional account of war by Karl von Clausewitz. For the latter, war is an outgrowth of the natural conflict between clearly-defined competing political policies of well-organized states. For Hobbes, in contrast, the condition of "war" is the natural condition of human agents apart from political institutions, dwelling in anarchy and in the absence of any discernable authority or rule of law.

In contrast to the customary hypothetical invocations by modern political philosophers, however, cyber conflict at present does not constitute some hypothetical "supposing" or fictitious "original position," affording a privileged vantage point for "reason" to adjudicate matters of fact. Rather, the cyber domain itself now confronts us with the first truly actual and accurate *instance* of such state or condition. A state of nature, accurately characterized by the *bellum omnium contra omnes,* is no more and no less what the cyber realm itself is.

In a fascinating sense, then, the cyber realm, with its many examples of conflict and lack of structure, also unintentionally provides us with the first authentic laboratory in which to examine the chief challenges and puzzle of the *Leviathan* itself: namely, how do civil society, social order and the rule of law manage to emerge from such a condition of primordial anarchy? After all, the underlying (if implicit) question in the *Leviathan* is: "what, in this miserable, fallen world of ceaseless conflict, are the prospects for peace?" And if it is peace, security, safety, as guaranteed through the rule of law that is the ultimate goal of the *Leviathan,* how is that goal to be attained?

For Hobbes the condition of "war" is the natural condition of human agents apart from political institutions, dwelling in anarchy and in the absence of any discernable authority or rule of law

When we, like Dr. von Wussow, invoke Hobbes descriptively, we are likewise obliged to consider the *normative* dimension in his investigations that is quite often forgotten. It is an admittedly thin moral conception for a philosopher famed for his rejection of morality otherwise, but it is a moral conception nonetheless: the obligation incumbent upon all who dwell within this state of nature (as Hobbes editorializes) "to quit it with the utmost dispatch." Confronted with our natural condition, he argues, we are not permitted to remain in it, but to transform it into something more stable and secure. On Hobbes's largely realist or "amoral" account, in point of fact, the sole action that would represent a genuinely moral or ethical decision beyond narrow self-interest would be the enlightened decision on the part of everyone to "quit" the State of Nature and enter into some sort of social contract that, in turn, would provide security through the stern imposition of law and order.

But here we encounter what might be termed the "reality paradox" in the cyber domain. Unlike Hobbes's fictional individuals languishing unpleasantly in a hypothetical state of nature, "law and order," let alone legal institutions like police, judges and courts, are precisely what the rank and file individual actors and non-state organizations (like "Anonymous") in the cyber domain *assiduously wish to avoid.* Hobbes's own solution to the problem of anarchy is likewise not one that any self-respecting cyber citizen would care to embrace: namely, that a well-regulated civil society will only be achieved through the forceful imposition of authoritarian rule. We have witnessed how nations like China currently attempt the Hobbesian formula in the cyber domain, with limited success. But that approach is not only anathema to democratic and rights-respecting societies – it would represent a fundamental betrayal of what we called earlier the natural virtues and limited natural rights valued by denizens of the cyber domain: liberty, anonymity, privacy, and behavior largely free from interference by others. There are no boundaries, and no governments in cyber space, and cyber citizens profess themselves unwilling to countenance, or yield to such impositions, whatever the Chinese government may attempt.[2]

A famous, if persistent problem with Hobbes is that the transition from anarchy to civil society is never really adequately explained. On the one hand, Hobbes appears to argue that the transition will occur pretty much as a matter of course, when inhabitants see their own self-interests optimized by sacrificing some of their freedom and rights in exchange for authoritarian-sponsored state security. But, at the same time, Hobbes recognizes that there is no guarantee that this benign transition will automatically occur. Some, the most malevolent in particular, will be resistant. The truly powerful, the strongest, in the state of nature will never willingly yield their personal authority to the rule of law, simply because it can never be, or be seen to be, in their own individual self-interest to do so.

The only moral imperative that Hobbes acknowledges is that the transition to civil society be made

In contrast to our "reality paradox" in the cyber domain above, this inconsistency generates what is generally known as the "Hobbesian paradox:" i.e., in order to achieve what would clearly be in the self-interests of all, *some act of force* must be utilized to override the narrowly-conceived self-interests of bullies and tyrants in the state of nature. Who, in the state of nature, will consent to dispatch the tyrants and bullies? And how may the rest of us retain confidence that any individual volunteer *willing* to do so, *will* do so without simply assuming their place? The moral imperative – the only moral imperative that Hobbes acknowledges – is that this transition to civil society be made. But apparently it cannot be made. Or at least, there is no clear path, nor ironclad guarantee, that it either can or will take place.

Emergent norms for cyber conflict

When we turn to cyber conflict from the perspective of international relations (IR), the malevolent actors are primarily rogue nations, terrorists and non-state actors (alongside organized crime). The reigning theory of conflict in IR generally is Rousseau's metaphorical extension of Hobbes from individuals to states: the theory of international anarchy or "political realism." There is one significant difference, however, between Hobbes and Rousseau on this condition of international anarchy. Although the "state of nature" for individuals in Hobbes's account is usually understood as a hypothetical thought experiment (rather than an attempt at a genuine historical or evolutionary account), in the case of international relations, by contrast, that condition of ceaseless conflict and strife among nations (as Rousseau first observed) is precisely what is actual and ongoing.

Conflict between international entities on this account naturally arises as a result of an inevitable competition and collision of interests among discrete states, with no corresponding permanent institutional arrangements available to resolve the conflict beyond the individual competing nations and their relative power to resist one another's encroachments. In addition, borrowing from Hobbes' account of the amoral state of nature among hypothetical individuals prior to the establishment of a firm rule of law, virtually all political theorists and IR experts assume this condition of conflict among nations to be immune to morality in the customary sense of deliberation and action guided by moral virtues, an overriding sense of duty or obligation, recognition and respect basic human rights, or efforts to foster the common good.

However we characterize conventional state relationships, the current status of relations and conflicts among nations and individuals within the cyber domain perfectly also fits this model: a lawless frontier, devoid (we might think) of impulses toward virtue or concerns for the wider common good. It is a "commons" in which the advantage seems to accrue to whomever is willing to do anything they wish to anyone they please whenever they like, without fear of accountability or retribution. This seems, more than conventional domains of political rivalry, to constitute a genuine war of all against all, as we remarked above.

Beginning in the summer of 2014, while working on my own study of cyber warfare,[3] I noted some curious and quite puzzling trends that ran sharply counter to expectations. Experts and pundits had long predicted the escalation of "effects-based" cyber warfare and the proliferation of cyber weapons like the Stuxnet virus. The major fear was the enhanced ability of rogue states and terrorists to destroy dams, disrupt national power grids, and interfere with transportation and commerce in a manner that would, in their devastation, destruction and loss of human life, rival conventional full-scale armed conflict. Those predictions preceded the discovery of Stuxnet, but that discovery (despite apparent U.S. and Israeli involvement in the development of that particular weapon as part of "Operation Olympic Games") was taken as a harbinger of things to come: a future cyber "Pearl Harbor" or cyber Armageddon.

But I began to notice that, by and large, this is not the direction that international cyber conflict had followed. Instead of individuals and non-state actors becoming more and more like nation-states, I noticed that states were increasingly behaving more and more like individuals and non-state groups in the cyber domain: engaging in identity theft, extortion, disinformation, election tampering and other cyber tactics that turned out to be easier and cheaper to develop and deploy, while proving less easy to attribute or deter (let alone retaliate against). Most notably, such tactics proved themselves capable of achieving nearly as much if not more political "bang for the buck" than effects-based cyber weapons (which, like Stuxnet itself, were large, complex, expensive, time-consuming, and all but beyond the capabilities of most nations).

In an article published in 2015,[4] I labeled these curious disruptive military tactics "state-sponsored hacktivism" (SSH), and predicted at the time that SSH was rapidly becoming the preferred form of cyber warfare. We should consider it a legitimate new form of warfare, I argued, based upon its political motives and effects. SSH, for example, perfectly fitted Karl von Clausewitz's aforementioned definition of warfare as politics pursued by other means. We were thus confronted with, not one but *two* logically distinct forms of cyber warfare: one waged conventionally by large, resource and technology-rich nations seeking to emulate kinetic effects-based weaponry; the second by clever, unscrupulous but somewhat less well-resourced rogue states designed to achieve the overall equivalent political effects of conventional conflict. I did not maintain that this was perfectly valid, pleading only (with no idea what lay around the corner) that we simply consider it: allowing that we might be mistaken in our prevailing assumptions about the form(s) that cyber conflict waged by the militaries of other nations might eventually take. We might simply be looking in the wrong direction, or over the wrong shoulder.

States were increasingly behaving like individuals and non-state groups in the cyber domain: engaging in identity theft, extortion, disinformation, and election tampering

And then the Russians attempted to hack the 2016 U.S. presidential election. The North Koreans proceeded to download the "WannaCry" software, stolen from the U.S. National Security Agency, from the "dark web" and used it to attack civilian infrastructure (banks and hospitals) in European nations who had supported the U.S. boycotts launched against their nuclear weapons program. Really! How stupid were we victims capable of being? SSH had become the devastating "weapon of choice" among rogue nations, while we had been guilty of clinging to our blind political and tactical prejudices in the face of overwhelming contradictory evidence. And we had been taken in, flat-footed, utterly by surprise.

At the same time, readers (of which there were not very many) and critics had been mystified by my earlier warnings regarding SSH. No one, it seems, knew what I was talking about! My editor at Oxford even refused me permission to use my original subtitle for the book: “Ethics & The Rise of State-Sponsored Hacktivism.” This analysis had instead to be buried in the book chapters. I managed, after a fashion, to get even! When the book was finally published in the immediate aftermath of the American presidential election in January of 2017, I thanked my publisher’s “publicity and marketing team:” Vladimir Putin, restauranteur Yevgeny Prigozhin, the FSB, PLA Shanghai Unit 61384 (who had stolen my personnel files a few years earlier, along with those of 22 million other U.S. government employees), and the North Korean cyber warriors, who had by then scored some significant triumphs at our expense. State-sponsored hacktivism had indeed, by that time, become customary practice.

The great puzzle for philosophers is, of course, how norms can be meaningfully said to “emerge?”

But where is the ethics discussion in all this? The central examination in my book was not devoted to straightforward mechanical application of conventional moral theory and reasoning (utilitarian, deontological, virtue theory, the “ethics of care,” and so forth) to specific puzzles, but to something else entirely: namely, a careful examination of what, in the IR community, is termed “the emergence of *norms of responsible state behavior.*” This, I argued, was vastly more fundamental than conventional analytic ethics. Such accounts are not principally about deontology, utility, and colliding trolley cars. They consist instead in a kind of historical moral inquiry that lies at the heart of moral philosophy itself, from Aristotle, Hobbes, Rousseau and Kant to Rawls, Habermas – and the book’s principle intellectual guide, the Aristotelian philosopher Alasdair MacIntyre.

The great puzzle for philosophers is, of course, how norms can be meaningfully said to “emerge?” Not just, “where do they come from, or how do they catch on,” but *how can such a historical process be valid,* given the difference between normative and descriptive guidance and discourse? Perhaps my willingness to take on this age-old question and place it at the heart of contemporary discussions of cyber conflict is why few have bothered to read the book! Who cares about all that abstract, theoretical stuff? We either want to discuss all the latest “buzz” concerning zero-day software vulnerabilities in the Internet of Things, or offer our moral analysis in terms of utility, duty, virtue and those infamous colliding trolley cars – merely substituting, perhaps, driverless, robotic cars for the trolleys (and then wondering, “should the autonomous vehicle permit the death of its own passenger when maneuvering to save the lives of five pedestrians,” and so forth).

Instead, I found it necessary to discuss the foundations of just war theory and the morality of exceptions or “exceptionalism” (i.e., how do we justify sometimes having to do things we are normally prohibited from doing?), as well as the IR approach to “emergent norms” itself, as in fact dating back to Aristotle, and his discussion of the cultivation of moral norms and guiding principles within a community of practice, characterized by a shared notion of the good. Kant, Rawls, and Habermas were invoked to explain how, in turn, a community of common practice governed solely by individual self-interest, may nevertheless evolve into one characterized by the very kinds of recognition of common moral values that Hobbes, as well, had implicitly invoked to explain the transition from a “nasty, brutish” state of nature to a well-ordered commonwealth – *precisely the kind of thing we are trying to discern now within the cyber domain.* Kant called this evolutionary learning process “the Cunning of Nature,” while the decidedly Aristotelian philosopher, Hegel, borrowed and tweaked Kant’s original conception under the title, “the Cunning of History.”

Finally, in applying a similar historical, experiential methodology to the recent history of cyber conflict from Estonia (2007) to the present, I proceeded to illustrate and summarize a number of norms of responsible cyber behavior that, indeed, seem to have "emerged, and caught on" – and others that seem reasonably likely to do so, given a bit more time and experience. Even the turn away from catastrophic destruction by means of kinetic, "effects-based" cyber warfare (as shrilly predicted by Richard Clarke and others) and toward SSH instead as the preferred mode of international conflict, likewise showed the emergence of these norms of reasonable restraint – doing far less genuine harm, while achieving similar political effects – not because we are "nice," but because we are clever, like Kant's "race of devils," who famously stand at the threshold of genuine morality.

This last development in the case of cyber war is, for example, the intuitive, unconscious application by these clever "devils" of a kind of proportionality criterion, something we term in military ethics the "economy of force," in which a mischievous cyber attack is to be preferred to a more destructive alternative, when available – again, not because anyone is trying to "play nice," but because such an attack is more likely to succeed and attain its political aims without provoking a harsh response. But such attacks, contrary to Estonia (we then proceed to reason) really should be pursued only in support of a legitimate cause, and not directed against non-military targets (I'm not happy about the PLA stealing my personnel files, but I am – or was, after all – a federal employee, not a private citizen). And the evolutionary emergence of moral norms, Kant's "cunning of nature," (or Hegel's "cunning of history") is thus underway. Even a race of devils can be brought to simulate the outward conditions and constraints of law and morality – if only they are "reasonable" devils.

Conclusion: the Hobbesian paradox

Once again, critics may view this account of emergent norms as being nearly as thin a conception of morality as that of Hobbes's attempt to encourage rogues and villains to embrace the rule of law. I cannot quarrel with this finding: morality is clearly treading on thin ice within the cold reaches of cyber space. But what is the alternative?

We would need to countenance an act of monumentally immoral proportions in response to the moral outrage most of us might feel at being held perpetual hostages in cyber space: our property, security, even our personal identities – as well as our public institutions and civil discourse and political decision-making – incorrigibly at risk to hijacking, theft, and corruption by unscrupulous persons, organizations, and rogue nations. This seems unacceptable, and so some act of intervention, forceful intervention, must be contemplated and ultimately attempted. But by whom, and upon what authority? Are all nations compelled to reassert national borders, and build virtual "firewalls" around them to keep out intruders (and to keep their own citizens and inhabitants in line)? This seems also unacceptable.

Either we acknowledge and nurture the fragile norms that grow up in the thin moral soil of cyber space, or else we colonize and tyrannize this new domain, forcing legal compliance at the expense of its most promising virtues.

[1] Miller, Seumas/Bossomaier, Terry (2019): *Ethics & Cyber Security*. Oxford (forthcoming).

[2] It bears mention that China, for its part, has accused the U.S. and western allies of attempting to impose its own form of hegemony on the "commons" that is the cyber domain, in exercises like the *Tallinn Manual on International Law* applicable to that domain. The official view is that cyber space is a "commons" in which all actors (individuals, collectivities, and nations) may act without restriction. That international view, however, is inconsistent with their domestic practice.

[3] Since published: Lucas, George R. (2017): *Ethics & Cyber Warfare*. Oxford.

[4] Lucas, George R. (2015): "Ethical Challenges of 'Disruptive Innovation': State Sponsored Hacktivism and 'Soft' War." In: *Evolution of Cyber Technologies and Operations to 2035*. Ed. Misty Blowers [Advances in Information Security, Vol. 63.] Basel, pp. 175–184.

The Author

George R. Lucas recently retired as the Distinguished Chair in Ethics in the Vice Admiral James B. Stockdale Center for Ethical Leadership at the United States Naval Academy (Annapolis), and as Professor of Ethics and Public Policy at the Graduate School of Public Policy at the Naval Postgraduate School (Monterey, CA). His most recent books include "Ethics and Military Strategy in the 21st Century: Moving Beyond Clausewitz" (2019), "Ethics and Cyber Warfare" (2017), "Military Ethics: What Everyone Needs to Know" (2016), and "The Routledge Handbook of Military Ethics" (2015).

OF CYBER, WAR, AND CYBERWAR

Authors: ***Eneken Tikk and Mika Kerttunen***

Abstract

Eneken Tikk and Mika Kerttunen introduce their essay with barely concealed irony. In a short prologue, the former describes her experiences on the day Estonia experienced a major cyber attack in 2007. The confusion caused by the outage of government and media websites disrupted many everyday processes. But even at the time, Tikk was surprised and somewhat dismayed by the largely uncritical use of terms like "war" and "self-defence" (though they are commonplace today). In fact, the situation was hard to classify from a legal or international law point of view. More than ten years later, the authors provide a clarification, which is still urgently needed. Rejecting the inflationary use of the term "war" – which apart from anything else plays down the horrors of an actual war – they advocate a definition of war that clearly follows Clausewitz. Neither current nor anticipated future cyber activities are subsumed by this concept, because – then as now, and most likely in the future – such activities are not capable of causing substantial physical damage. The fact that militaries around the world are developing and expanding their capacities to wage war via electronic means does not contradict this observation. Rather it is a logical consequence of increasing digitalization and interconnectedness. Nevertheless – and this is the authors' central argument – this issue is about more than just terminology. As cyberspace becomes a zone of conflict, talk of war makes us blind to actual risky developments. Because of their "below-the-threshold" character, cyber operations of all kinds are attractive as a standard means of projecting power – especially to smaller states and new cyberpowers. This promises to bring destabilization, the gradual debasement of the principles of international law, and escalatory automatisms leading to the risk of a conventional kinetic war.

Prologue: cyber odyssey 2007

Let's begin with a war story; certainly there are war stories also in cyberwar; this one is Eneken's:

"I am a survivor of the First Cyberwar. I may even be a veteran. Of the latter I am not entirely sure.

Cyber bombs fell on Estonia in the end of April 2007. Nobody saw the bombers or heard the bombs falling, but everybody learned of their arrival when the defence minister, speaker of the parliament, minister of justice, and the prime minister all assured us they were there. Suddenly, the riots on the streets seemed secondary to this war. Weapons of mass destruction had hit us. We were under a blockade. Russia, the gargantuan eastern neighbour had (finally) made its move.

The tiny Tallinn airport was operational the next morning. I had no choice but to leave – there was a working meeting on personal data protection in Brussels and my orders to participate had not been withdrawn. Well, nobody had called me to postpone the trip, and had there been any 'normal' orders, I would not have known as there was no access to the governmental information system.

I took off with a heavy heart. What should you pack when departing from a war zone? My grandparents had buried the family valuables in the garden when they left their home during the Second World War. That seemed a little unhelpful as I had nothing of that kind. Valuables, I mean.

In Brussels, the technocratic work was hardly on my mind. I kept checking the Estonian news, with no success: no online media site would open, and government websites were also down. However, everyone at the EU Commission and our colleagues from NATO were reporting the war.

After a day filled with a constant flow of breaking news, I took a taxi to the airport. After checking in, I felt a little more at ease. There still was a country to go back to. I felt grateful and relieved – whatever was going to happen the next day, I would face it with my family and friends.

The next day at the office – I had two jobs – I learned what it means to be part of the public administration of a country at war. Not that anything directly threatened my so far comfortable life, but it was still a chaotic situation: an immediate legal assessment of the situation was required; hourly technical updates were requested; talking points kept pouring in; phones were ringing constantly.

Preparing my legal assessment of the situation, I felt how unprepared I was to deal with the notion of war. Not only was I unable to apply any rules of international law to the situation, but I kept circling back to municipal, national law; the penal code, data protection requirements, even the public information act that had made it easy to simply copy and paste hundreds of email addresses from the ministries' websites straight into the "weaponized code." When I spotted an international lawyer saying that international law is not fully equipped to deal with the type of war Estonia was in the middle of, it made some sense. However, this memo also suggested that international law was to be developed to deal with such attacks. I was not entirely sure of this – but then again, I had no educated opinion.

I also noticed our chief of defence saying in the corridors that nothing that was going on had any military significance. He must have been wrong. I was not sure how or why, but it was clear that the situation was nothing short of conflict as the Ministry of Defence was deeply involved. The NATO Centre of Excellence was to remain involved. I was to remain involved. So, clearly, the chief of defence must just have been confused: we now had a very different type of war to wage that did not exist when he was taught what for and how to fight.

The next day, the war was over. Naturally, the cyberattacks became a keen object of research at the Centre. We, the scientists and researchers, suddenly got to attend countless meetings – Brussels, Mons, Redmond, prominent UK and US universities, and think tanks – to tell our story, the story of a new kind of war.

At one of those many panels, somebody mentioned Estonia having invoked the right of collective self-defence under Article 5 of the North Atlantic Treaty. This was news to me, so I decided to check it out. Indeed, NATO had received a letter from Estonia warning against cyberattacks that, in our expertise and best assessment, were likely going to be a threat to all NATO countries.

"We did NOT invoke Article 5," I wrote in my notes. To fortify my talking points, I added: "No country can invoke collective self-defence if there is no armed attack. Some states regard this threshold to coincide with that of use of force, but the Estonian incident was nowhere near to any such threshold."

Apparently, I was slightly misguided again. Months later, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was fully operational with not three members as per the minimum requirement, but seven! Estonia was the go-to country for cyber defence advice and cyberwar stories. The UN First Committee took up the issue of international cybersecurity and Estonia occupied one seat in the group of initially 15, then 20 and then 25 experts to attend to this issue.

Years later, when I analysed national positions on international law on this matter, I discovered that until 2006, as is obvious from the UN First Committee archives, Russia was the only country to sponsor the narrative of information and communications technology (ICT) as a theatre of war in the UN. Now, cyberwar is all around us. Much of it is very reminiscent of what fell on Estonia in 2007. It still does not make a lot of sense to try to apply laws of war to it. We should (much) rather ask ourselves if a solid resilience plan and better cyber hygiene, also on behalf of government institutions, could be more useful in this situation: cybersecurity starts at home.

Now, cyberwar is all around us. It still does not make a lot of sense to try to apply laws of war to it

Oddly, I feel like a veteran. I feel like a veteran of the war that never happened but that created a narrative of war that suddenly is becoming normalcy."

*

Never let a good crisis go to waste – the saga of 2007 has been helpful to the control-freak East, the operations-savvy West, the insecure

South, the unsure North, the eager industry, and the well-meaning peace lovers. We have heard many loud statements and seen many capitalized attributes witnessing cyberwar being waged. We do not believe in these testimonies.

Of war

It's true that bad, harmful, and malicious things take place in cyberspace. Children are being bullied, exposed, and exploited, online fraud and theft appears to be easy and profitable, videos of violence are roaming free, and states, the civilized members of the international community, are conducting mass surveillance and targeted intelligence (espionage) and some destructive operations. But war? Let's get real.

It's true that we can detect a lot of 'wars' going on. While we have, hopefully, got rid of the notorious notion of the 'Global War on Terrorism,' another nonsense notion, 'hybrid war' has entered the theatre scene. Some time ago we waged protocol and browser wars, cola wars and coke wars; the war on obesity that humankind is constantly waging but is sure to lose. Agreed, the notion of war, perhaps similarly to *jihad,* is being used in a colloquial and expressive way to enrich the argument: something crucial and important is going on. But, if everything is war, the horrors of real war are being diminished and mainstreamed. If war is being waged everywhere, human and societal life is reduced to constant state of conflict. Most importantly, if we believe in the ongoing or looming war in cyberspace, we had better get ready to wage it. That is what many governments are proposing.

We strongly advise that the expression of war only be used when speaking about organized state violence – the use of it against another state or politically organized entity

We strongly advise that the expression of war only be used when speaking about organized state violence – the use of it against another state or politically organized entity. The wording is less important than the idea behind it. War is organized, that is, the conduct of war, warfare, waging of war, is organized and purposeful, politically motivated, systemic and systematic. War is violent, that is, it causes death and destruction. War belongs to the property of states; individuals resorting to violence are criminals. War also can also be seen as a phenomenon which takes place in an armed battle between states; yet, both the structural and phenomenological approximations follow the same logic.

We can also justifiably talk of *civil wars (Sic!), intifada* and insurgencies, wars of liberation, where one of the fighting parties is a state and the other, not necessarily having the formal status of a state, an organized group operating as a political entity. The political character of *fronts, armies,* and *organizations* of liberation, even tribes, is obvious: the political character does not require a parliament or parties but rather desires, set objectives, and thought-out means and measures to achieve the ambitions. Harold Lasswell's 1936 book titled *Politics. Who Gets What, When, How* made this clear straightaway. If a politically organized and motivated entity is conducting systematic and organized death and destruction-causing violence against another similar entity, let's face it: it is a war. Legally, this may not be the case, but then, legally, very few wars have been waged since the Korean War (which, by the way, has not yet formally ended).

Our approximation of war is Clausewitzian. Despite the changes in its colours and structures – the famous chameleon argument – the nature of war as violent, uncertain, and purposeful remains. The current and anticipated state of cyber activities and operations, even by states, does not fit these criteria.

Of cyber

Cyber operations have not caused large-scale destructive effects. Communications have been blocked, web pages have been smudged, electricity has been shut off, information has been destroyed, industrial systems have been halted, and financial and identity losses have been suffered. Yet there is very little smoke and rubble, and, most importantly, no human casualties. In fact, almost any other human activity is more lethal than cyber operations.

Most importantly, cyber effects, ranging from manipulation to denial of access and services to degradation and destruction of information and systems are not likely to cause such second- and third-level effects that would make states resort to war. Cyber operations do not threaten the existence of states or shackle the balances of power, they do not create wider, long-term, and decisive effects that military campaigns and war proper aim for and can achieve. In the brutal reality of political decision-making, the question is not one of the conceptual possibility of death and destruction, but the scope of violent, devastating, and painful effects.

Why then are many nations nevertheless developing cyber military capabilities, establishing cyber-specific units and commands, training and educating personnel to conduct cyber operations, and waging war in cyberspace? For example, since 2012, the USA has been systematically reviewing its national strategies, joint military doctrines, and field manuals to incorporate cyber capabilities as an elementary part of all military operations and functions. This would also include deploying cyber units and teams to tactical land forces formations, perhaps “down” to manoeuvre brigades, integrating cyber capabilities into the full range of military operations. Russia and China are trying to incorporate tools of information warfare into their military forces. The tree-hugging Nordics are building up capacities of cyberwarfare, and Estonia, *et tu,* a nation of barely over one million inhabitants, established a cyber command in November 2018. What’s that, *militarization?*

Armed forces have always been at the forefront of employing the latest information and communication technologies. Computers were originally used to, well, compute. What was established next, as early as the 1950s, was connectivity between surveillance stations, command posts, and fire and manoeuvre units. In the aftermath of the Cuban missile crisis, the USA established (an ill-functioning) “Worldwide Military Command and Control System.” Digitization has improved the accuracy of targeting. Currently, the majority of armed forces are modernizing their command and control and weapons systems. Looking for better effects and better ways to achieve effects, the most advanced are integrating their systems and networks. Smart and connected technologies are being deployed and employed to all military functions, administrative and lethal. Everyone is trying to protect their data and networks.

Cyber capabilities are certainly being used in all contemporary conflicts. Governments employ cyber means in political and economic espionage, too. Some are also said to conduct criminal activities online. A conceptually correct and factually accurate notion to explain and entertain the development, deployment, and employment of ICT and cyber military capabilities is *cyberwarfare,* a combination of ways and means, methods, and capabilities, tools and their use.

Precisely their falling short of war makes cyber operations lucrative and dangerous. They have been proposed as the default form of power projection. Some countries are openly proud of their cyber capabilities and operations, perhaps thinking them to be risk-free. The opposite is true.

Conflicts and contestation are nevertheless not virtual per se but political and real. Even the purest form, the most romantic image of cyber operations – exchanges of virtual salvos and hasty coding – does not take place in isolation or at the speed of light.

The logic of war and politics and the reality of cyber operations thus leave us in a paradoxical situation: as long as cyber operations are only capable of causing relatively minimal, temporary, and secondary effects, they are not elevated to the level of war. Cyber operations causing serious existential or destructive effects (which is unlikely), would escalate the situation to traditional political and military conflict and war.

Some countries are openly proud of their cyber capabilities and operations, perhaps thinking them to be risk-free. The opposite is true

Statistically, the vast majority of known or suspected state-sponsored cyber incidents constitute acts of espionage. The rest few dozens of recorded incidents result in relatively minor effects, such as defacement of websites, denial of services, manipulation of data, and in very limited instances, data destruction, sabotage, and physical consequences. The situation as such is far from anything war-like.

The problem

The obsession with cyberwar makes us miss the point of what *is* going on. The cyber militarization surge does not involve only known and established powers – between them, cybernetics may become a way to avoid unnecessary casualties and destruction. We see whole new operational identities emerging in all continents; within the EU especially in Estonia, the Netherlands, and Poland.

The entrance of the cyber newbies to the global conflict theatre is alarming and potentially destabilizing. Their presence testifies to an appetite for becoming relevant by power projection. Despite acknowledging that development and use of these capabilities positions them in the danger zone of their adversaries, new cyber powers let their operational ambitions take over their commitment to the rule of law. Just a little, it seems – a nip on sovereignty and a tuck on due diligence. These cuts, however, are serious wounds to the public international rule-based order. A self-proclaimed right to deny sovereignty of one nation denies the right to sovereignty of all.

Development of new operational capabilities feeds the *perpetuum mobile* of political tensions and easily leads to an unwanted or unanticipated escalation. In any case, there is no way to predict how these newly found powers will develop or how resistant the new cyber powers are to political manipulation and provocation. Accordingly, while we are admiring the cyberwar that isn't, we miss developments that might lead to an actual conflict.

The habit of conducting cyber operations is a risky business. The climate of cyber conflict and the (mis)perception of cyberwar further destabilizes the delicate balance between normalcy and crisis. During a cyber situation, political decision-making is easily inflicted by sense of urgency, the primacy of hard security, and the fallacy of appearing powerful. Yet decisions are made amidst a fog caused by misinformation, miscalculation, uncertainty, and fear. National and organizational exercises celebrate escalatory language and measures. De-escalation seems to be too difficult even to think about, but that is precisely what is needed.

We all hope this time will not come. We all know it likely will. We don't know how many cuts it takes for the international order to fatally bleed. Human rights, the rule of law, and the leitmotiv of peace are all neglected in the cyber power game. Voluntarism brings out the lack of the sense of accountability in the community of states. It underlines that states, unlike social communities, are not bound by any shared identity or common values. Instead, it reminds that the only common denominator between states is their political self, and that the prospect of any global governance is a mere utopia.

This brings us to another kind of nonsense – voluntary and non-binding norms of responsible state behaviour, the placebo offered to the international community as a substitute to international law. Because there is no prospect of war between them, the United States and the Russian Federation can afford to dance a slow waltz with each other in the ballroom of no restraint. In their heavy hug, they are too self-confident and comfortable to deal with the overwhelming lack of resilience, awareness, and accountability looming all over the world. Tallies of new cyber powers are considered allies to one and excuses for the other – until the carriage turns back into a pumpkin.

The world has been just peaceful enough for states to drop their guard. There is, however, a real prospect of conflict in ICT if its development and use are not taken seriously. This prospect is not cyberwar. It is the prospect of real war. The type of war that international humanitarian law was made for.

The Authors

D.Soc.Sc Mika Kerttunen *and* ***D.Jur. Eneken Tikk*** *are founding directors of the Cyber Policy Institute and senior research scientists at Tallinn University of Technology. Mika and Eneken are experienced in cyber diplomacy and capacity-building. They have also served as advisors to their national (Finnish and Estonian, respectively) experts at the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.*

Books

Clausewitz, Carl von (1991 [1832]): *Vom Kriege.* Cologne.

Lasswell, Harold (1936): *Politics. Who Gets What, When, How.* New Haven.

Libicki, Martin C. (2012): *Crisis and Escalation in Cyberspace.* Santa Monica. https://www.rand.org/pubs/monographs/MG1215.html (accessed May 20, 2019).

Rid, Thomas (2013): *Cyber War Will Not Take Place.* London.

Skinner, Quentin/Stråth, Bo (2003): *States and Citizens.* Cambridge.

Tikk, Eneken/ Kerttunen, Mika (2018): *Parabasis: Cyber-diplomacy in Stalemate.* Oslo. http://hdl.handle.net/11250/2569401 (accessed May 20, 2019) .

Tikk-Ringas, Eneken (2016) (ed.): *Evolution of the Cyber Domain.* Abingdon.

Articles

Arquilla, John/and Ronfeldt, David (1993): "Cyberwar is Coming!" In: *Comparative Strategy* 12 (2), pp. 141–165.

Kerttunen, Mika (2018): "Cyber Warfare – from Science Fiction to Reality" In: *Sicherheit und Frieden* 36 (1), pp. 27–33.

Libicki, Martin C. (2015): "The Cyberwar that Wasn't." In: Geers, Kenneth. (ed.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn, pp. 49–54. https://ccdcoe.org/uploads/2018/10/Ch05_CyberWar-inPerspective_Libicki.pdf (accessed May 20, 2019).

Raitasalo, Jyri (2019): "America's Constant State of Hybrid War." In: *The National Interest,* https://nationalinterest.org/feature/americas-constant-state-hybrid-war-48482 (accessed May 20, 2019).

Others

Council on Foreign Relations: "Cyber Operations Tracker." https://www.cfr.org/interactive/cyber-operations (accessed May 20, 2019).

NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/ (accessed May 20, 2019).

RISKY WAR GAMES:
WHY WE CAN ONLY LOSE IN THE CYBERWAR

Author: ***Anke Domscheit-Berg***

Abstract

As the internet finds its way into all areas of modern life, it seems hard to imagine that originally, in 1968, it was a military project to network a few computers together. Having brought this fact to the reader's attention, Anke Domscheit-Berg notes that the idea of "active cyber defense" suggests a remilitarization of the internet. Cyberspace is becoming a war zone, she argues, where cyber weapons are added to the military's arsenal. At the same time, people around the world are subject to surveillance by security services, as we have known since Edward Snowden's revelations. Played down as merely a normal means of modern defense, calls for "active cyber defense" and for "hackbacks" by the state are growing louder in Germany, as elsewhere. Yet in the author's view, such instruments are incompatible with the German constitution. Not only that, but the risk of escalation with such activities is massively underestimated: uninvolved persons could be affected all too easily. It is extremely difficult to separate civilian and military targets in cyberspace.

So there is only one way to make us all safer in the digital age, and that is to ensure that software and hardware are as secure as possible. But this is at odds with the desires of the intelligence services and armed forces. They highly prioritize surveillance opportunities and cyber attack capabilities. For this reason, says the author, once new software and hardware weaknesses are identified, they are often systematically and secretly left open. In this way, the state itself becomes a security risk.

Finally, Domscheit-Berg advocates transparency in software and hardware development, and comprehensive digital education. After all, as she puts it, people are still "one of the biggest weaknesses."

The roots of the internet go back to 1968, when the ARPANET computer network began to be developed in partnership between the U.S. Department of Defense and Massachusetts Institute of Technology. ARPANET initially connected a handful of research facilities that were working for the U.S. military. Creating a network of computers and transmitting information by splitting it into small packets of data are the basic principles on which the internet still operates today. ARPANET was funded by the Defense Advanced Research Projects Agency (DARPA), which is under the control of the U.S. Department of Defense. DARPA's main task is to promote research activities useful to the military, with a focus on basic research. Created at the end of the 1950s, DARPA now has an annual budget of more than three billion dollars.[1] Some of the research funded by DARPA still shapes the digital world today – the TCP/IP internet protocol, for example, and the invention of the mouse. Other projects were focused on aerospace, such as satellite development, and very many were used by the military: from the air force (e.g. detection avoidance for airplanes, drones), to the navy (anti-submarine warfare, unmanned underwater vehicles), and other armed forces (M16, anti-tank weapons, helmet displays, autonomous weapons, field robots.)[2]

From military technology to the digital society

Over the following decades, what we now know as the internet came into being. At first it was mainly an academic network. It was not until 1994 that more people used the internet commercially than for science and research. Since then, the internet has broken free of its military roots. It became the foundation of the digital society, the starting point of a digital revolution. New business models were created, and with them countless small enterprises but also incredibly large and powerful companies – the ones we now refer to as GAFA, the quasi-monopoly of Google, Amazon, Facebook and Apple. The world's knowledge became accessible at the click of a mouse, while billions of people could network and communicate with each other directly. In 2017, Facebook had 2.3 billion users, 1.9 billion people shared or watched videos on YouTube, and 1.5 billion people sent chat messages, photos or videos to each other on WhatsApp.[3] Today, a single smartphone has more computing power than the NASA Apollo Moon mission had in its day, it could navigate 120 million Apollos simultaneously to the moon.[4] Whichever aspect you look at, we are increasingly entering dimensions that are hard to imagine. In 2022, around 4.8 zettabytes of data will be transmitted over the internet.[5] One zettabyte is 1,000 to the power of seven bytes, equivalent to one trillion gigabytes or a one followed by 21 zeroes. While data volumes and the number of networked devices are growing exponentially, prices are falling through the floor: one gigabyte of storage space in 1981 cost 500,000 U.S. dollars; in 2017 it cost just 3 cents.[6]

The remilitarization of cyberspace

In this networked big-data society, a noticeable remilitarization has been happening for some time. Cyberspace is becoming a war zone, cyber weapons are being added to the military's arsenal, and the desires of the intelligence services have not only grown, but are realized on a worrying scale. Thanks to NSA whistleblower Edward Snowden, we have all been able to take a look through an unexpectedly opened window into an otherwise closed world. We have glimpsed the almost limitless extent of global surveillance of internet and communication traffic by U.S. intelligence services. We all remember the months when one shockwave after the other rolled through the media, as new, inconceivable dimensions of spying were discovered. Along with industrial espionage between supposedly friendly countries, even Angela Merkel's mobile phone was tapped. And the German intelligence services were involved too. Investigative committees subsequently busied themselves with explaining what had happened, but no legal or personal consequences resulted from the illegal surveillance activities. Instead, they were legalized after the fact[7] – e.g. the grossly disproportionate tapping of Germany's largest internet exchange point DE-CIX in Frankfurt am Main.

Quite obviously, parliamentary oversight completely failed, and not least because it is structurally impossible for it to work. The power relations are just too unequal. Desires for new powers are constantly announced, police laws are extended, new cyber institutions are created, "active cyber defense" is mentioned ever more frequently – which of course is no longer defense, but an attack, even if it is called a counter-attack. Germany's interior minister, Horst Seehofer, has repeatedly supported this option in the form of "hack-backs" by the state. This would be contrary to international law, and also incompatible with the German constitution: defense is a matter for the *Länder* and not the task of intelligence services, the military or any other federal institutions. It is highly irritating that even the President of the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik,* BSI), Arne Schönbohm, desires a hack-back capability.[8] The BSI's competences extend only to IT security, prevention, and providing assistance in the event of hacker attacks.

> ***Quite obviously, parliamentary oversight completely failed***

The state becomes a digital attacker

"Hacking back" by the state is not the same as a conventional military counter-strike in the event of an attack. One problem is the difficulty of attribution, i.e. the ability to reliably identify an attacker. With a long-range missile, you can tell with absolute certainty which country it was launched from, which is not possible with a hacker attack. No intelligence service in the world can say with 100% certainty where a cyber attack originated. The possibilities for camouflage are too diverse, false tracks are laid too often, "signatures" of known hacker groups are imitated, or third-party servers are used for attacks, without their owners knowing anything about it. In the best case, you might have clues and suspicious facts, but you cannot be certain.

Let us just imagine that a hack-back of this kind is carried out. A server in another country is attacked from Germany, because it is thought to be controlled by criminals. But what if the server is in a hospital? Or in a government building? What if the attack forces schools to close or causes a power outage? What would an attack like this mean if the country was correctly identified, but the perpetrators were criminals acting on behalf of a different country, or completely independently? What if we attacked servers in a third country that had absolutely nothing to do with the whole affair? You only have to imagine this crazy approach in the context of conventional warfare to see how dangerous and absurd it is. We do not go and bomb a third country because an individual terrorist perpetrator or member of a terrorist group ("probably") comes from that country or only traveled through that country on their way to carry out a terror attack.

The threat to our civilization as a whole is comparable to the impact of climate change, only even less predictable

Any third country attacked in this way could discover the unjustified hack-back. They might then suspect that it was done by Germany, and in turn interpret it as an attack – especially if critical infrastructure was hit or if the hack-back got out of hand because malware used for the attack had spread. An escalating spiral could now be set in motion, and there is no reason it would have to remain limited to two countries or to cyberspace. We should not even entertain the idea of playing with fire like this. It is potentially more dangerous than a nuclear war. If this comparison seems exaggerated, it is worth reflecting on just how many things around us today are connected to the internet. Just consider all the places that software is installed, and the areas of society and industry that would suffer dramatic consequences if there were a partial or total IT failure. For hospitals, traffic management systems, electricity networks and power plants, government agencies and many businesses, it would be a major disaster. If cyberspace, containing all these civilian institutions, becomes a theater of war, there is no longer any separation between civilian and military parties in a conflict. There would be too many victims, and the conflict could escalate and spread at terrific speed, since the internet knows no national borders.

Sadly, we have apparently not realized yet that the only winning move in a cyberwar is to not to play this kind of war game in the first place – as was vividly demonstrated in the movie "War Games," by the computer that simulates a nuclear war.

But it is not just hack-backs by the state that pose a danger. All potential players – state and non-state – are capable of creating malware that compromises all our security, whether with criminal intent or for surveillance purposes. Nuclear weapons are in the hands of only a few countries. They cannot be acquired by other countries without threat of sanctions, and their production requires so many resources that the barriers to acquisition are very high. In contrast, there is no comprehensive ban on cyber weapons or digital weapons, and the resources required to develop them are orders of magnitude smaller. The danger is great because it has become so much easier to carry out an attack, and at the same time the potential impacts have become much greater. It is conceivable that hacker attacks could essentially catapult us back to the Middle Ages, if this Pandora's box is ever opened.[9] The threat to our civilization as a whole is comparable to the impacts of climate change, only even less predictable.

There is only one sensible conclusion that can be drawn from this realization: we should do everything we can to make our IT systems more secure. But what we find instead is an immoderate attitude, devoid of ethical boundaries, that has lost sight of the big picture. Intelligence services see only the surveillance potential that a digitalized society offers them. They imagine how nice it would be if they could not only wiretap phone calls, but also eavesdrop on virtual assistants like Alexa and Siri, if they could hack into the Internet of Things and bug fridges, toasters and washing machines. They want surveillance software built into cars, so that not only can they track someone who moves from A to B, but also know who is in the car with them, and what they are talking about.[10]

State surveillance fantasies

I grew up in East Germany, and I remember the Stasi. When I was a student, my letters were opened, my dorm room with a typewriter in it was searched. I lived knowing that I was being watched, and from my own experience I know that there can be no freedom with surveillance, because if you are under surveillance, you are not free. Mass surveillance is not compatible with democracy. It is the tool of totalitarian systems seeking to prolong their existence by controlling their populations. Yet security services in all countries have an inherent desire always to know more, to collect and analyze as much data as possible, even if they are in a democratic country. Their dream is to have a transparent population while maintaining their own complete obscurity to the greatest possible extent. As the devil flees holy water, so they shy away from parliamentary oversight. Yet this is a necessary safety net for our democracy. Its purpose is to draw clear boundaries for intelligence activities, in line with our democratic values. The activities of the NSA just show too clearly that this description is not an Orwellian delusion. The potential dangers of mass surveillance, too, are completely different today than during the *Stasi* era, when the world still largely ran on analog technology and there was no Facebook, WhatsApp, cookies on websites or Internet of Things.

Alongside the intelligence services, the desires of the armed forces in Germany are also growing; and increasingly often they are working hand-in-hand and sometimes even together with the police. In 2017, the Central Office for Information Technology in the Security Sphere (*Zentrale Stelle für Informationstechnik im Sicherheitsbereich,* ZITiS) was set up. This new institution will ultimately be located at the Bundeswehr site in Munich. Its main tasks include breaking encryption, investigating social networks in real time, and telecommunication surveillance. On its advisory board, the German Federal Police (*Bundespolizei*), Federal Criminal Police Office of Germany (*Bundeskriminalamt,* BKA), German Federal Intelligence Service (*Bundesnachrichtendienst,* BND), Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*) and the German Military Counterintelligence Service (*Militärischer Abschirmdienst,* MAD) jointly determine its work program.[11] This composition violates the separation of powers between the police and secret services, which was established after the terrible experience of the *Gestapo* regime during the Nazi period. Parliamentary oversight of ZITiS is practically impossible, since it does not lie within the competences of the Parliamentary Oversight Panel (Parlamentarisches Kontrollgremium, PKGr) set out in the Act concerning parliamentary oversight of intelligence activities (Parliamentary Oversight Panel Act (Kontrollgremiumgesetz, PKGrG)), nor is it subject to general parliamentary scrutiny: answers to specific questions by the Left Party group in the Bundestag were refused, because as classified information they could not even be lodged in the parliamentary Secret Records Office (Geheimschutzstelle).[12] ZITiS is therefore located in an oversight gap. Close involvement with the military is also evident from the fact that the agency offers study sponsorships at the University of the Federal Armed Forces.

> ***Mass surveillance is not compatible with democracy. It is the tool of totalitarian systems***

ZITiS is set to employ 400 people by 2020. Meanwhile there is a shortage of security experts in the jobs market, which represents another security problem. In October 2018, the first 81 vacancies at ZITiS were filled, but three out of every four persons employed had been poached from other jobs in government. Only one in four came from the "open market." ZITiS offers higher salaries, on average, than other government agencies. In early 2019, according to published recruitment advertisements,[13] starting salaries in telecommunication surveillance[14] are higher than those at the BSI.[15] If cyber security experts at a government agency designed to attack are better paid than at an agency tasked with defense, one can imagine what will happen and what impacts that will have on the quality of our defense capabilities.

Another example of the militarization of cyberspace in Germany is the creation of a cyber agency (formerly ADIC). This agency for innovation in cyber security will be established in the Halle-Leipzig region in 2019, and employ around 100 people. The German federal government has said very clearly that this facility to support cyber research projects will function in a way similar to DARPA in the United States, and has approved a budget of 200 million euros over the first five years. In the words of defense minister Ursula von der Leyen, the cyber agency should act as a "'treasure hunter' [...] in the military and civilian sector"[16] and cooperate with all cyber bodies of the *Bundeswehr:* the Cyber Innovation Hub in Berlin, the Cyber and Information Domain Service (*Kommando Cyber- und Informationsraum,* KdoCIR), and – like ZITiS – also with the cyber security degree program at the University of the German Federal Armed Forces in Munich.[17] Even though this institution was set up jointly by the German Federal Ministry of the Interior (*Bundesministerium des Innern,* BMI) and Federal Ministry of Defense (*Bundesministerium der Verteidigung,* BMVg), it is obvious that it is really under the control of the *Bundeswehr* and BMVg. Having said that, in the field of IT security there is an explicit intention to link internal and external security more strongly,[18] in other words, to bind the military and intelligence services more closely together. This is a worrying prospect, as then a cyber deployment of the *Bundeswehr* within Germany becomes possible, which should be just as much of a no-go as any other military deployment of the Bundeswehr inside Germany. To enable it to pay higher salaries, the cyber agency was granted an exemption by the German finance ministry, and as a result – just like ZITiS – it attracts important IT security and defense experts, luring them away from other government bodies. And, like ZITiS, the cyber agency too completely escapes any kind of parliamentary oversight, since it was formed as a limited company (GmbH), like any public sector enterprise.

We will not be able to control the growing risks in a digitalized society unless we concentrate fully on defense

Defending digital security

We will not be able to control the growing risks in a digitalized society unless we concentrate fully on defense. The times are long past when we were only talking about computers or cellphones. In a few years, there will be 50 billion networked devices[19] in the world, from smart meters and fitness watches to self-driving cars. With its exponential growth, particularly the Internet of Things confronts us with major challenges in respect of IT security. Many products have a very poor security level, with no or inadequate password protection, zero or insufficient maintenance via software updates, and numerous security flaws that are open like a barn door. It is simply too much to expect consumers even to assess the risks associated with buying these kinds of products, particularly since in most cases the risks are not transparent because the necessary information is not provided.

It is also owing to this very frequent poor product quality that an extension of product liability to IT manufacturers is overdue. It should cover precisely the kind of damage caused, for example, by a smart toaster that becomes part of a malicious botnet due to inadequate IT security.

According to BSI, there are already more than 600 million known types of malware, with another 280,000 or so being added every day. In 2016, around 1,000 vulnerabilities were known in the ten most frequently used software products alone.[20] Anyone who builds up attack capabilities, i.e. hacking skills, is intentionally harming all our IT security, since you can only hack IT systems if you exploit security flaws instead of fixing them. But there are no good security flaws that let us monitor terrorists, and bad security flaws that expose the rest of society to hacking risks; there are just hardware and software security flaws in general, which expose anyone to a risk who uses a device with that hardware or software. For this reason, the danger for us all increases every time an intelligence service discovers a security vulnerability – or buys one on the black market, using taxpayers' money – so that they can use it themselves for hacking later on.

The state as a security risk

According to press reports, the BND itself was given a budget of 4.5 million euros for the period from 2015 to 2020, to buy security vulnerabilities.[21] The National Security Agency (NSA) in the United States received more than 25 million dollars for the same purpose in 2013. We gained an impression of the risks this practice entails, in 2017, when criminals used the WannaCry malware worm – which exploits a security flaw in Windows – as part of an extortion scam. The NSA had already known about the security flaw for five years, but kept it secret – and so more than 230,000 computers in 150 countries got infected. Among those hit were the telecommunications company Telefónica, the British National Health Service, the Romanian foreign ministry, and 450 computers at German railway operator *Deutsche Bahn,* knocking out one regional control center and many display boards.

What is needed, instead, is a strict ban on government agencies buying information on previously unknown vulnerabilities, and a mandatory general duty to report security flaws – which of course must also include weaknesses discovered by the intelligence services. There should be an international ban on the security vulnerabilities trade. In its place, other incentives can be created that make it attractive to find and report security flaws.

Our armed forces should be purely a peace army that relies on defense, not offense, even if the country is under attack. At any rate, an "active cyber defense" is inconceivable without developing attack capabilities and without increasing the general security risks. Moreover, considering the uncertain attribution of cyber attacks, it also amounts to a kind of "self-defense just in case" against a state to which the attack is attributed – which is completely impermissible under international law.

International humanitarian law also clearly prescribes a principle of distinction: military attacks may only be directed at military targets, not at civilians or civilian property. With hack-backs, it is impossible to predict exactly what kind of target you are actually attacking. High civilian collateral damage therefore cannot be ruled out. It is also not clear who in Germany is actually supposed to carry out these hack-backs. But if the cyberwar capabilities of the *Bundeswehr* are to be used, this raises the additional issue of the requirement for parliamentary approval. After all, it would seem unrealistic to expect an attack by government hackers on a foreign target to be openly debated in parliament beforehand. When interior minister Seehofer addressed the *Bundestag's* Committee on the Digital Agenda, in the context of his desire to legalize hack-backs via an amendment to the constitution, he mentioned that such decisions "may have to be taken within a few minutes." In this case, the *Bundestag* could definitely not give the required approval of *Bundeswehr* deployments.

There should be an international ban on the security vulnerabilities trade

Transparency and digital education for greater digital security

It is right to invest in IT security and IT security research, but the focus should be on defense. That includes a clear expansion of the development and use of open-source software and hardware, because in an ever more complex, digitally networked world, transparency and traceability are increasingly important conditions for greater security and trust. Open products allow a look inside. They are not black boxes, where back doors can be especially well hidden. Open source is not more secure per se, but its verifiability increases the likelihood of vulnerabilities being found, and also fixed. We should place a greater emphasis globally on chips and software that have longer development cycles, but for that reason are more reliable and verifiable. “Security by design and security by default”[22] should be the guiding principle for all IT products, although state regulation setting minimum standards for IT security is also needed. These standards should include minimum update obligations for software, as well as password protection worthy of the name for networked devices, so that poorly chosen passwords like “123456”, “qwerty” or “password” are not accepted. The fact that millions of these passwords are used is not just down to users. Irresponsible product design is also to blame.

But people themselves are actually one of the greatest weaknesses. So there is a need for more lifelong education and training programs – which should be easily accessible and include all sections of society – to improve basic IT security skills. Too often, we naively plug an unknown USB stick into our own or the company’s computer. Too many times we click on links in phishing emails, or use an easy-to-guess password. All too infrequently do we encrypt our emails, protect social network accounts with two-factor authentication, or regularly install software updates. The BSI should be expanded, for this purpose too, as a national consumer protection authority. Better prevention across the country is an important step in the right direction. Greater security for us all requires engagement by all of us – politicians, business people, scientists and civil society.

I very much hope that it does not take a catastrophic event to make us understand that we can only make our infrastructure and the foundations of the digital society more secure by acting together – and together also means that we stop thinking about IT security in terms of national borders.

The Author

Foto: Jesco Denzel

Anke Domscheit-Berg (51) is a publicist, an internet activist, and a Member of the German Bundestag. For the DIE LINKE parliament group, she is spokeswoman for network policy, chairwoman of the Committee on the Digital Agenda, and a deputy member of the Artificial Intelligence Study Commission. After nearly 15 years at Accenture, McKinsey and Microsoft, she went freelance in 2011. She has authored several books, publishes in numerous media, and is a regular public speaker in Germany and other countries. Designing a digital society for the common good is her main focus..

[1] "Budget." https://www.darpa.mil/about-us/budget (accessed March 28, 2019).

[2] "A Selected History of DARPA Innovation." https://www.darpa.mil/Timeline/index.html (accessed March 28, 2019).

[3] "Ranking der größten sozialen Netzwerke und Messenger nach der Anzahl der monatlich aktiven Nutzer (MAU) im Januar 2019 (in Millionen)." https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user/ (accessed June 6, 2019).

[4] Puiu, Tibi (2019): "Your smartphone is millions of times more powerful than all of NASA's combined computing in 1969." https://www.zmescience.com/research/technology/smartphone-power-compared-to-apollo-432/ (accessed June 6, 2019).

[5] "Cisco Visual Networking Index: Forecast and Trends, 2017-2022 White Paper". https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html (accessed March 28, 2019).

[6] Klein, Andy (2017): "Hard Drive Cost per Gigabyte." https://www.backblaze.com/blog/hard-drive-cost-per-gigabyte/ (accessed March 28, 2019).

[7] "BND darf am Internetknoten weiter Daten abzapfen." https://www.spiegel.de/netzwelt/netzpolitik/de-cix-betreiber-von-internet-knoten-verliert-klage-gegen-bnd-a-1210243.html (accessed March 13, 2019).

[8] Unger, Christian (2018): "Hackerangriffe kann man sich wie eine Pizza bestellen." https://www.morgenpost.de/politik/article215355473/Hackerangriffe-kann-man-sich-wie-eine-Pizza-bestellen.html (accessed March 28, 2019).

[9] Marc Elsberg describes such a scenario very impressively in his novel *Blackout – Tomorrow will be.* https://en.wikipedia.org/wiki/Blackout_(Elsberg_novel) (accessed May 27, 2019).

[10] Linder, Roland et al. "Auch die Geheimdienste wollen mit Alexa spionieren." https://www.faz.net/aktuell/wirtschaft/diginomics/geheimdienste-wollen-alexa-offenbar-zur-ueberwachung-nutzen-16136726.html (accessed May 23, 2019).

[11] Deutscher Bundestag, Drucksache 19/6246 (2019): „Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. André Hahn, Gökay Akbulut, Anke Domscheit-Berg, weiterer Abgeordneter und der Fraktion DIE LINKE [The Federal Government's reply to a minor interpellation by Dr. André Hahn, Gökay Akbulut, Anke Domscheit-Berg and other members of parliament and the group DIE LINKE]." Berlin. http://dipbt.bundestag.de/dip21/btd/19/062/1906246.pdf (accessed April 1, 2019).

[12] Ibid.

[13] See therefore job offers of the ZITiS on: https://www.zitis.bund.de/DE/Karriere/Stellenangebote/stellenangebote_node.html (accessed April 1, 2019).

[14] Biselli, Anna (2018): "Statt Mate: Hackerbehörde ZITiS findet nicht genug Personal und probierts mit 2.000 Koffein-Shots." https://netzpolitik.org/2018/statt-mate-hackerbehoerde-zitis-findet-nicht-genug-personal-und-probierts-mit-2-000-koffein-shots/ (accessed April 1, 2019).

[15] "Tabelle TVöD Bund, gültig vom 1. März 2018 bis 31. März 2019." https://www.bsi.bund.de/SharedDocs/Stellenangebote/DE/Entgelttabelle.pdf?__blob=publicationFile&v=6 (accessed March 28, 2019).

[16] "BMVg und BMI geben Standort für neue Cyberagentur bekannt [BMVg and BMI announce location of new cyber agency]." https://www.bmvg.de/de/aktuelles/standort-fuer-neue-cyberagentur-30534 (accessed March 28, 2019).

[17] "BMVg und BMI geben Standort für neue Cyberagentur bekannt." https://www.bmvg.de/de/aktuelles/standort-fuer-neue-cyberagentur-30534 (accessed March 28, 2019).

[18] "Bundeskabinett beschließt Cyberagentur." https://www.bmvg.de/de/aktuelles/bundeskabinett-beschliesst-cyberagentur-27392 (accessed March 28, 2019).

[19] "Prognose zur Anzahl vernetzter Geräte weltweit in den Jahren 2003 bis 2020." https://de.statista.com/statistik/daten/studie/479023/umfrage/prognose-zur-anzahl-der-vernetzten-geraete-weltweit/ (accessed May 13, 2019).

[20] Steiner, Henning (2017): "Die Lücke der Software: Wie eine Hackerin ins System kommt." https://www.hr-inforadio.de/programm/dossiers/die-luecke-in-der-software-wie-eine-hackerin-ins-system-kommt,schwachstellen-in-software_einfallstor-fuer-hacker-100.html (accessed March 28, 2019).

[21] Voss, Oliver (2017). "Erpressersoftware 'WannaCry': Sicherheitslücken auf der ganzen Welt." https://www.tagesspiegel.de/wirtschaft/erpressersoftware-wannacry-sicherheitsluecken-auf-der-ganzen-welt/19806608.html (accessed March 28, 2019).

[22] Security by Design: Development of products and services, with a state of the art security level.
Security by default: the basic setup of a product has to be as secure as possible, which excludes default access passwords like "0000" or "admin."
See: Hahn, André (MdB) et. al. (2018). Fraction THE LEFT. in the Bundestag (ed.). "Cybersicherheit" – ein Beitrag für einen sicheren digitalen Raum [Cyber security" – a contribution to a secure digital space]." p. 12. https://www.linksfraktion.de/fileadmin/user_upload/180709_Digitale_Sicherheit.pdf (accessed May 23, 2019).

CYBER SECURITY AND CYBER DEFENSE

GREATER PROTECTION THROUGH INTERMINISTERIAL COLLABORATION

Abstract

Given the increasing threat scenarios originating in cyberspace, it is becoming increasingly important for states to incorporate cyberspace into their national security architecture. In 2016, the Federal Republic of Germany drew up a cyber security strategy that is designed to take present and future threats into account. The strategy mentions military aspects of cyber defense, stating that the defense capabilities of the German armed forces in cyberspace are a "key part of cyber security architecture." Thus, according to the author, the establishment of the Bundeswehr Cyber and Information Domain Service (Kommando Cyber- und Informationsraum, KdoCIR) is an excellent strategic move for German cyber security.

Since the Bundeswehr relies on critical civilian infrastructure to maintain its operational readiness, the author argues that it is appropriate to develop effective mechanisms to protect this infrastructure even in peacetime. Könen's essay briefly discusses the legal and organizational bases before detailing the need for close cooperation between different departments. The threat situation in cyberspace simply has to be dealt with collectively. As the security situation becomes more complex, technical evaluations of cyber activities have to be viewed in context with the foreign policy and military situation, in order to provide a comprehensive assessment of the danger.

For the most extreme case – Könen emphasizes this – the technological capability should be available to isolate or completely shut down attacker systems. He believes this is a necessary condition for active cyber defense, and it would be important to specify threshold criteria and establish decision-making processes. But the necessary debate has only just begun.

Author: ***Andreas Könen***

In 2016, Germany's federal government approved a Cyber Security Strategy for Germany. Action area 3 sets out criteria and guiding principles for an "Effective and sustainable national cyber security architecture" (translated from German). The key strategic goal and measure is to strengthen the defense aspects of cyber security. Thus the corresponding paragraph of the cyber security strategy states that the priority aspects of cyber defense are a military part of overall defense in cyberspace: "The defense capabilities of the Bundeswehr in cyberspace are [...] an essential part of the cyber security architecture. The close relationship is demonstrated both by the overlap in content regarding the technical implementation of protection measures, and by the use of and active participation in the structures, processes and reporting systems of cyber defense in ways and situations that are relevant to defense."[1]

In April 2017, the German Federal Ministry of Defense (*Bundesministerium der Verteidigung,* BMVg) set up the Cyber and Information Domain Service (*Kommando Cyber- und Informationsraum,* KdoCIR). This was a significant strategic move, and had been announced in the cyber security strategy. It is therefore worth taking a new look at the strategic goals and measures that were described in 2016, relating them to current developments in cyber policy, and perhaps drawing new conclusions. This particularly applies to the interaction between civilian and military cyber security measures in the areas of protecting critical infrastructures, the threat situation in cyberspace, international cyber security policy and active cyber defense.

Protecting critical infrastructures

Special attention has been given in recent years to protecting critical infrastructures. A legal framework for protecting critical supply infrastructures has been created with the German IT Security Act (IT-Sicherheitsgesetz) of 2015, the resulting "Ordinance for determining critical infrastructures in accordance with the German Federal Office for Information Security Act" (*Verordnung* *zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz,* BSI-KritisV), and the EU's Network and Information Systems (NIS) Directive. Legislators are using a twin-pronged approach to promote cyber and information security. Firstly, they are imposing an obligation on businesses to produce, implement and audit company-specific information security concepts. This preventive approach will ideally be supported by creating an industry-specific minimum standard that businesses can use for guidance, which has already been taken up by the insurance industry, for example. The second part of the approach is intended to assist detection and response. By introducing a duty to report cyber security incidents, legislators have established the basis for producing a cyber security situational overview for critical infrastructures across all industries and sectors.

The draft German IT Security Act 2.0 represents a next step to protect prominent companies in Germany. The existing supply-critical approach is being extended e.g. to the waste disposal industry and the culture and media sector. In addition, the concept is being modified so that the regulations now also apply to businesses that, as a result of advancing digitization, are dependent on information technology to a greater degree than others. This would be the case if a cyber attack could paralyze their business activities, for example, or even cause large-scale damage. A new term, "IT-critical enterprises," has been coined for these businesses. But just being IT-critical would not in itself be a sufficient reason for regulation. Only if a special significance affecting the community as a whole becomes apparent does the state have a duty of care to protect these enterprises, ultimately for the benefit of citizens. Good examples of the need for regulation of this kind include the chemical industry, due to its potential for large-scale harm, the defense and security industry in its role as a supplier to the Bundeswehr and other security agencies at federal and state level, the auto industry because of its importance for the economy as a whole with regard to IT in production planning and control systems, and also businesses that have substantial knowledge and expertise requiring protection (intellectual property).

So where, within the whole civilian topic of cyber security for critical infrastructures, do we find the link to the structures of military defense? Let us consider the extended concept of critical infrastructures that includes IT-critical enterprises having an importance for society as a whole. Now it immediately becomes clear that the *Bundeswehr* and its supply industry can absolutely be identified as critical infrastructure in this sense – even in peacetime. This is immediately evident from the digitization and interconnectedness of the armed forces in general, the use of highly complex IT in weapons systems, the automation of mobile vehicles and aircraft, and a fully digitized communication and command infrastructure. Conversely, in peacetime and in a state of defense, the *Bundeswehr* depends on the functioning of civilian critical infrastructures in the extended sense stated above. The availability of national and international telecommunications and the national and international internet are prime examples.

By introducing a duty to report cyber security incidents, legislators have established the basis for producing a cyber security situational overview for critical infrastructures across all industries and sectors

Because the German Federal Ministry of the Interior (*Bundesministerium des Innern,* BMI) is responsible for public security and the security of supply to the population in peacetime, and because the BMVg and *Bundeswehr* need recourse to the critical infrastructures in a state of defense, a new challenge arises in terms of the sharing of tasks and responsibilities between both departments, including in the event of threats and attacks from cyberspace. A careful analysis and assessment of the respective IT dependencies on critical infrastructures and their interdependencies is therefore essential for internal and external security, even in a state of peace. This particularly applies to crisis and disaster preparedness, and ultimately also to a state of defense. Pre-coordinated response mechanisms should be derived from these considerations and rehearsed in advance.

Specifically, this concerns coordinated or even identical information security requirements for IT products or for the cyber security of network or communication infrastructures (those used jointly or, for example, under NATO). Many of these requirements are already being drawn up and put into practice, e.g. in approval procedures adopted by the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik,* BSI) in connection with classified information, or in planned procurements for IT consolidation at federal level. Here the BSI's new IT baseline protection *(IT-Grundschutz)* methodology with user-specific profiles for cyber security requirements is the tool of choice, also for the *Bundeswehr*.

A common approach to the standardization of cyber security requirements in European and international standardization bodies is desirable

But given the steady advance of digitization, new action areas are constantly arising – for example the cyber security of products in the Internet of Things, or communication via (virtual) networks with different security levels. Thus there is already a wealth of possible research approaches for the Agency for Innovation in Cyber Security *(Agentur für Innovation in der Cybersicherheit)* that is being jointly set up by BMVg and BMI. In addition, however, a common approach to the standardization of cyber security requirements in European and international standardization bodies is also desirable.

The threat situation in cyberspace and how to deal with it collectively

The National Cyber Defense Center (*Nationales Cyber-Abwehrzentrum,* CyberAZ) was established by BSI in 2011 as a cooperation and coordination platform. From within BMVg's area of responsibility, CyberAZ is assisted particularly by the Cyber and Information Domain Service (*Kommando Cyber- und Informationsraum,* KdoCIR). KdoCIR works together with the other federal security agencies, the German Federal Office of Civil Protection and Disaster Assistance (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,* BBK), but also the critical infrastructure supervisory authorities. It exchanges information, analyses and assessments relating to the cyber situation. Based on this information sharing, the work of CyberAZ has the following main goals: coordinated operational handling of cyber security incidents, producing the dynamic national cyber security situational overview, and providing the authorities involved with coordinated and practiced crisis response mechanisms for a cyber crisis. There are plans to potentially expand CyberAZ to include the German federal states and private sector.

New challenges arise for CyberAZ at the interface between civilian and military defense. CyberAZ's cyber security situational overview is based in large part on the findings of civilian bodies such as the computer emergency response teams (CERT) in various authorities and other institutions. The sources used generally reflect a situation in the national and international networks that is characterized by a wide variety of cyber security incidents of a civilian nature, which are mainly attributable to cyber crime, cyber espionage, or cyber sabotage. Military cyber security scenarios do not fall within the task spectrum of the authorities concerned. Naturally they come under the responsibility of KdoCIR, within its own structures. The military cyber security situational overview is produced there, too. In the past, a differentiation between civilian and military cyber security scenarios could be derived from the embedding of cyber security incidents in security events in the physical world. But this clear distinction is no longer possible.

Cyber security incidents in the recent past demonstrate that we can expect an increase in cyberspace incidents with a hybrid character. Cyber attacks can be and increasingly are used below the threshold of military attacks in scenarios of inter-state diplomatic or political crises. They increase the complexity of the cyber security situation. A consistent and comprehensive analysis and assessment of such incidents, taking all aspects into account, can therefore only be carried out in cooperation between KdoCIR, BSI and the other agencies in CyberAZ. Of course one specific challenge in assessing hybrid attacks is to combine the technical assessment by CyberAZ with the assessment of the foreign-policy and military situation. Here it particularly falls to BMVg, the German Foreign Office (*Auswärtiges Amt,* AA), German Federal Chancellery (*Bundeskanzleramt,* BKAmt) and BMI together with their subordinate authorities to facilitate and structure cooperation and coordination with the respective situation centers.

Suitable preparations should also be made for a possible state of defense, so that all information on the civilian cyber security situation can be passed on to the *Bundeswehr* and KdoCIR in a crisis that is escalating into a state of defense. The necessary structures, legal bases and processes built on them are still only at an incipient stage, however.

International cyber security policy

Close collaboration between BMVg and BMI, and between KdoCIR and BSI, also plays an important role in terms of Germany's active positioning in European and international cyber security policy. This is especially true of the measure entitled "Developing NATO's cyber defense policy" (translated from German). Here is another passage from the 2016 cyber security strategy:

"As a cornerstone of Germany's security and of Euro-Atlantic security, the North Atlantic Alliance relies on adequate protection against attacks from cyberspace in order to fulfill its core tasks, especially in the area of collective defense and in international stabilization deployments. The goal is to continuously increase the overall resilience of the Allies and of the Alliance, and to increase deterrence and defense capabilities not least in the context of hybrid threats."[2]

What is largely unknown, however, is the fact that BSI constitutes both the German NATO Crypto Security Authority (NCSA) and NATO Cyber Defense Authority (NCDA), and therefore represents Germany in various NATO bodies together with KdoCIR or BMVg. In historical development terms, this mainly reflects the fact that in the context of protecting classified information, BSI is responsible for national approvals of military communication equipment, and also contributes its expertise as part of corresponding NATO approval bodies. Logically, then, the role of the BSI was extended to the corresponding issues in cyber security (here the same as cyber defense), mainly in networks.

For NATO, in defense situations, it will be essential for the Member States to have suitably robust and reliable critical infrastructures in place

Now we need to consider the position with regard to further future developments. For NATO, in defense situations, it will be essential for the Member States to have suitably robust and reliable critical infrastructures in place, especially the network infrastructures that would be needed in a state of defense. Therefore, alongside the national and European cyber security requirements formulated above, corresponding requirements should be specified by NATO and implemented at national level. To ensure the availability of resilient networks both in civilian crisis or disaster scenarios and in a state of defense, it is necessary to coordinate the requirements resulting from the German IT Security Act with those from NATO. KdoCIR and BSI should cooperate more closely in the future to coordinate these requirements, which currently still exist loosely alongside each other.

Civilian and military aspects of an active cyber defense

At the present time, means of civilian defense for use in civilian crises or disasters in cyberspace – which take the form of cyber sabotage against critical infrastructures, with corresponding impacts – are being discussed under the term "active cyber defense." In the case of national defense, collective defense within NATO, or an overseas deployment, active defense measures can be deployed in cyberspace if a corresponding authorization is given by the German *Bundestag* for a deployment of the *Bundeswehr* or the powers of KdoCIR. For civilian active cyber defense measures, however, relevant legislation is still needed.

Furthermore, there is a need to develop the corresponding capabilities, in the first place for civilian defense measures in cyberspace based on the relevant authorizations. Enhanced protection for national infrastructures against cyber sabotage attacks from outside Germany could be achieved in the first instance e.g. by blocking (parts of) the internet, specifically blocking the attackers, and by the respective provider isolating the targeted systems. Inside Germany, if a crisis or disaster situation was detected in the national part of cyberspace, it is conceivable that BSI could have powers to issue orders and take action as a regulatory authority. BSI could assist the federal and state police forces with police emergency response activities, and also cooperate with police forces in other countries to ensure that attacker systems located there are neutralized.

In the most extreme case, for defense purposes, it should also be possible to deactivate attacker systems via active cyber defense measures, for example if imminent danger necessitates a response in the shortest possible time. Suitable decision-making processes in this regard would then also need to be established.

Yet even setting up a civilian active cyber defense, as outlined above, leaves complex questions unanswered. Hybrid threat scenarios, for example, where it is no longer possible to draw a sharp distinction between sabotage and military attacks, are a common method of destabilizing the victim in the “analog world” of today. Similar scenarios are all the more conceivable, and in many different forms, in the virtual world. Attackers could combine destabilizing activities in the analog world with cyber sabotage and thus create a double hybrid threat situation – civilian versus military and analog versus digital.

Solutions or approaches to such complex defense scenarios do not yet exist today. They require more in-depth analysis and assessment. This represents another field for extensive cooperation between military and civilian authorities in Germany, and with our partners abroad, particularly in the EU and NATO. Aside from resolving questions relating to international law and emergency response legislation, developing appropriate technical, organizational and political solutions, and creating suitable crisis response mechanisms, there is also a need for fundamental discussions about ethical standards in the digital and cyber world. This discussion has only just begun.

[1] Bundesministerium des Innern [German Federal Ministry of the Interior] (2016): *Cyber-Sicherheitsstrategie für Deutschland 2016* [Cyber Security Strategy for Germany]. Berlin, p. 33 (translated from German). https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (accessed 26. April 2019).

[2] Ibid., p. 40 (translated from German).

The Author

***Andreas Könen** holds a degree in mathematics and is Director-General CI – Cyber and Information Security in the German Federal Ministry of the Interior, Building and Community (BMI), where he previously held the position of head of Directorate IT II – “IT and cyber security; secure information technology,” and ÖS III – “Cyber security in the field of law enforcement and domestic intelligence.” From 2006 to 2016 he held various managerial positions at the German Federal Office for Information Security (BSI); most recently he was Vice President. Prior to that, he performed various roles within the German federal administration, with a focus on information technology. Andreas Könen is married and has two children.*

THE GERMAN CYBER AND INFORMATION DOMAIN SERVICE AS A KEY PART OF NATIONAL SECURITY POLICY

Author: ***Lieutenant General Ludwig Leinhos***

Digitalization is the dominant cultural and social feature of the present age – it is the megatrend for the 21st century. Digitalization and virtually limitless networking are enabling enormous improvements and innovations. Processes and communication are made faster and more efficient. Life has become easier and more convenient in many ways. When is the next bus coming? Is it going to rain tonight? Quickly turn the heating down at home, from a smartphone. Technological progress is facilitating all aspects of everyday life and society.

Digitalization has become a priority issue in the German armed forces as well. Even today's weapons systems such as the Eurofighter or a warship are reliant on digital sensors, networks and computerized decision support systems. Logistics chains would be almost unmanageable without IT systems, and even the future infantryman will increasingly be a digitized sensor and effector.

The integration of cutting-edge IT into military planning and decision-making processes has a decisive impact on modern armed forces operations. It also increasingly determines command and control procedures as well as leadership culture.

Challenges of digitalization

Yet for all the benefits and achievements, there is another side to the coin: digitalization has created new dependencies and vulnerabilities. Many states and businesses regard risks from cyber space as one of, if not the largest threat in the years and decades ahead. Cyber attacks on states, critical infrastructure and private homes have long been a reality. Attacks happen every day, are automated or highly sophisticated, and ever more ambitious. Many of us vividly remember the impacts of the WannaCry and NotPetya malware, or the attack on the Berlin-Bonn Information Network (IVBB) at the end of 2017. States, businesses and private individuals are all targeted. For businesses, even low-threshold cyber attacks can cause damage costing billions. At the end of 2018, it became clear just how much our private lives could be affected, too. A school student with no formal IT training collected large amounts of personal data from various people who had not sufficiently protected their online privacy, and uploaded it on Twitter where it was publicly accessible.

Along with attacks from cyber space, activities in the information environment are also on the rise – such as fake news campaigns. These are deliberately aimed at provoking unrest. Inter- and intra-state conflicts are increasingly influenced by propaganda and disinformation. Information is becoming a core resource of the future.

These trends will intensify in both quality and quantity. Adequate protection is therefore of fundamental importance for state, economy and society. The state must ensure it can maintain its capacity to act while protecting and providing for the population. The capabilities of the *Bundeswehr* in the cyber and information domain can make a significant contribution in this regard.

Set-up of the *Bundeswehr* in the cyber and information domain

Ever since the 1990s, the *Bundeswehr* has devoted a lot of attention to IT security. For over 20 years, it has operated its own IT security organization with around 600 personnel. It places a particular emphasis on awareness of IT-related issues among its members. In response to the impacts of increasing digitalization, the new Cyber and Information Domain Service was set up in April 2017. It bundled existing units and has developed their relevant knowledge and expertise, and will continue to do so.

The new Service has a highly diverse portfolio of tasks. One focus of its activities is on protecting and operating the German armed forces' IT systems in Germany and abroad. Another is on strengthening and developing intelligence, surveillance and reconnaissance (ISR) and effects capabilities in the cyber and information space. This includes cyber operations such as infiltrating enemy IT networks, electronic warfare, and operational communication on deployments abroad. Geoinformation service staff support the whole range of *Bundeswehr* operations in mission accomplishment by providing all kinds of high-resolution, quality-assured digital geospatial information. In addition, the Cyber and Information Domain Service by exchanging information and cooperating with other national and international institutions contributes to national security provision and strengthens Germany's cyber security architecture.

The German Cyber and Information Domain Service Headquarters has already established its own situation centre for the cyber and information space domain. A valid situation picture, providing the basis for options for action and synergies, is generated by merging available situation reports from all areas relevant to the cyber and information domain. Analysts process different types of structured and unstructured data from a variety of sources. In the future, they will use artificial intelligence and big data methods. For example, correlating data from *Bundeswehr* IT systems with military intelligence as well as publicly available information from social networks could lead to conclusions being drawn relating to an increasing hybrid threat or a coordinated cyber attack. We make these analyses available to users in the *Bundeswehr* and other agencies. We have also recruited new specialists for the *Bundeswehr* Cyber Security Centre. The Cyber Operations Centre was established on April 1, 2018, and was followed a year later by the *Bundeswehr* Centre for Software Expertise on April 1, 2019. All of these activities have brought us a good step closer to achieving our self-imposed goal of shaping all aspects of the cyber and information domain in an integrated way.

Special features of the cyber and information domain

Since the 2016 Warsaw Summit, NATO has regarded cyber space as an independent theatre of operations – along with land, air, sea and space. In cyber space, armed forces can use special software to reconnoitre enemy systems, and take action against them. Specifically, for example, logistics chains can be interrupted, vital data for operations can be modified, and command and information systems can be disabled. In the German armed forces, we deliberately define this new military domain even more broadly than NATO to include the information space. Beyond technology, this is where information is perceived, interpreted and spread by humans. So-called "publicised opinion" is one of the important aspects that we focus on.

> *Our activities have brought us a good step closer to achieving our self-imposed goal of shaping all aspects of the cyber and information domain in an integrated way*

The cyber and information space has several special features compared to the other conventional theatres of operations. It is characterized by a high degree of complexity. Territoriality is complemented by virtuality. It cannot be divided into zones of action with clear geographical boundaries. The same applies to troop manoeuvres. It is certainly possible, however, to achieve physical effects in the cyber and information space, by all means. But the locus of impact of cyber and information space operations may be thousands of miles away from the source of activity. Time, too, has a different meaning. After all, in cyberspace, effects can be achieved over any distance with no time delay, and in real time.

The attribution of attacks is problematic. Technological possibilities allow activities to be disguised especially well. There are also many potential types of perpetrators and motives. Owing to the opportunities of digitalization, non-state actors by means of cyber attacks can achieve effects now that were previously the preserve of state actors. Digitalization has made hazard assessment much more complicated. It is always necessary to know: Who is attacking us and with what aim? In this context, the issue of attribution, with its technical, legal and political aspects, gains a special importance. In collective or even national defence scenarios, binding international rules – similar to those that apply to armed conflicts between states – must also be applied to the cyber and information space.

Consequences of digitalization

Change in the form of military conflict

Increasing digitalization has important implications in terms of conceivable military scenarios. A future conflict scenario will be essentially characterised by hybridity, the waging of conflict in the digital realm, artificial intelligence, and autonomy. The intensity of actions may intentionally remain below the accepted threshold required to classify them as armed attacks. This reduces the probability of classic military confrontations between industrial nations, and makes hybrid forms of conflict more likely. Conventional military forces of sufficient quality and quantity still have to be kept ready, however, to ensure a credible deterrent.

Increasing digitalization reduces the probability of classic military confrontations between industrial nations, and makes hybrid forms of conflict more likely

Cyber and information space operations – either carried out autonomously or supportively – gain further importance. They are conceivable as first-hour operations, possibly even before "conventional forces" have been alerted. After all, inter- and intra-state conflicts are already being increasingly influenced by propaganda and disinformation. In the future, armed forces will need to be more sophisticated and more specialized. New thinking is needed for operations in the cyber and information space that form an independent area of operations, yet also provide support as part of classic military land, air or sea operations. We must develop capabilities for cyber and information space operations over the full spectrum, so that we can offer policymakers options for non-kinetic action.

Consequences for organization and processes

Increasing digitalization has an impact on all kinds of areas within the armed forces. At the same time, of course, the *Bundeswehr* tries to exploit the benefits of digitalization to the greatest possible extent. Apart from command and weapons systems, potential applications exist, for example, in personnel management, logistics, energy management and in producing situation pictures and forecasts.

Organization has to adapt to the requirements of digitalization. This is not about providing IT support for existing processes, but rather of adapting and optimizing processes based on the possibilities of digitalization. We need new strategies as an integrated national approach to the hybrid conflict scenario I described earlier. Do we need an adjustment of rules and powers at the national level to enable an adequate response to the "digital state of defence"?

Furthermore, the ethics of digital conflict must be discussed by society as a whole, and within the *Bundeswehr*. In my view, there is an absolute need to create binding international rules. The law of war needs to be adapted to modern forms of conflict. We need to find an international consensus on the application of key ethical terms, among others, such as "suffering" and "attack", to the cyber domain. For guidance, we should look to the ethical standards that have proven effective as a basis for existing international law. A good foundation has existed since 2017 in the form of the *Tallinn Manual 2.0.*

We must also consider ethical aspects, especially in relation to weapons systems. A responsible approach to new technologies is mandatory. Not everything that is technically possible should necessarily be implemented and legitimized. This also applies to the field of artificial intelligence.

Consequences for leadership, command and control procedures, training and "culture"

Command levels and command and control procedures have to be reviewed and adapted. In the future, a comprehensive situation picture and automated recommendations for action will increasingly coincide at higher levels. The issuing of orders and their implementation in hierarchies must be reconsidered against this backdrop. In general, we are confronted with the following questions: Are tools and processes from the past still right for today? Could modern tools such as Design Thinking offer alternative approaches?

Digitalization will also alter the profile of the military profession. We need a digital organizational culture in the armed forces. The cultivation of cyber awareness among all members of the *Bundeswehr* is of elementary importance, as is the development of a cyber security culture. The digital age calls for different skills than those required during the Cold War era. This has to be taken into account in leadership as well. We must allow and reflect on innovative thinking, and not suppress it under pressure to conform. Rapid cross-hierarchy communication must become an accepted and established practice. And of course, with regard to the recruitment process and career paths, the armed forces must be more flexible so that they can attract and retain urgently needed talent.

The Cyber and Information Domain Headquarters has already adjusted to the new circumstances. We see ourselves as a major driver of digitalization-related development in the *Bundeswehr*. Within our organisation, we explore new and innovative paths, implement faster processes – for example using special collaborative software – and encourage independent initiative. We do this by embarking on new procedures and principles in cooperation, which makes us a pioneer for the *Bundeswehr* as a whole.

Essential for protection against the challenges of digitalization

Close national and international cooperation

The internet has no natural boundaries. Effects and attacks can hit everyone: states, businesses and private individuals. Close national and international cooperation is therefore essential for effective protection against dangers from cyber space.

National cooperation is based on the German Federal Government's Cyber Security Strategy, which was adopted in 2016. It places responsibility for cyber security on the German Federal Ministry of the Interior. The 2016 White Paper states that defence aspects of the national cyber security architecture are originally tasks of the German Federal Ministry of Defence, and are constitutionally assigned to the *Bundeswehr*. It is the task of security and defence policy to ensure the territorial integrity and sovereignty of Germany and its allies.

> *The digital age calls for different skills than those required during the Cold War era. This has to be taken into account in leadership as well*

Hybrid strategies use interfaces between responsibilities – e.g. between domestic and foreign security – to achieve their goals. Close cooperation and dialogue in the national setting are therefore extremely important. Back in 2011, the National Cyber Defence Centre was created under the guidance of the German Federal Office for Information Security. It serves as a forum for cooperation between government bodies in the cyber and information domain. The centre is currently being developed into an interministerial, operational institution involving all key stakeholders – a crucially important step to ensure Germany's future capacity to act in this field. It is imperative that internet service providers are involved too. The Cyber and Information Domain Service is making an active contribution to this process as a representative of the *Bundeswehr*. As the National Cyber Defence Centre develops, we could provide information from our new joint situation centre, for example.

The Cyber and Information Domain Service is already closely networked with all key authorities and government agencies. We have also entered into our first partnerships with academic and business institutions – for instance, there is a partnership with Deutsche Telekom, and an IT security alliance with the Fraunhofer Institute for Communication, Information Processing and Ergonomics. In both cases, the goals of cooperation are a general exchange of information and knowledge transfer, an exchange of personnel via reciprocal job shadowing, and the opening up and facilitation of mutual training and further education opportunities for IT professionals. In addition, the Cyber and Information Domain Service Headquarters is a member of the advisory board of the Cyber Security Cluster Bonn e.V., which was set up at the end of last year.

The Cyber and Information Domain Service is already closely networked with all key authorities and government agencies

Close dialogue is essential at the international level too, since the cyber and information space is not a respecter of national boundaries. In the military sector, there is already very close bilateral cooperation, as well as at EU and NATO levels. Transfers of knowledge and expertise have now been established with corresponding NATO agencies, along with participation in joint forums. Joint exercises at strategic and operational levels take place at regular intervals.

Conclusion

Having discussed the various aspects, it becomes clear that digitalization has already had a significant impact on the *Bundeswehr,* and will continue to do so into the future. The associated challenges require new solutions and approaches in many areas. We must face up to these additional opportunities and resulting military scenarios, and prepare ourselves accordingly. Successful cyber defence is a strategic issue for government, business and society. One important requirement in this regard is to install binding international agreements that address the specific features and fast pace of the cyber and information space. Among the key aspects here are, not least, international law and ethics.

Only together can we guarantee resistance to threats from the cyber and information space – an essential requirement for the future of modern societies. The Cyber and Information Domain Service of the *Bundeswehr* will make a substantial contribution to this important national task, and assist with all resources available to it.

The Author

Ludwig Leinhos *(born 1956) joined the Bundeswehr in 1975. After gaining a degree in electrical engineering, the Lieutenant General (Generalleutnant) in the German Air Force had assignments in intelligence gathering and reconnaissance/electronic warfare. During his military career, he took on various leadership roles in Germany and abroad, in the areas of command systems and IT planning & application. His positions included that of Director NATO Headquarters C3 Staff in Brussels. General Leinhos became the first Chief of the Cyber and Information Domain Service (Inspekteur Cyber- und Informationsraum, InspCIR) on April 1, 2017.*

"THERE IS NO MILITARY OPERATION, NO MILITARY CONFLICT WITHOUT A CYBER DIMENSION TODAY"

Interview with
Major General José Luis Triguero de la Torre

In the 2018 Brussels Summit Declaration NATO reaffirms its determination "to employ the full range of capabilities, including cyber, to deter the full spectrum of cyber threats." Just for understanding: How does deterrence look like in cyberspace?

In a broader sense, NATO defines deterrence as "convincing a potential aggressor that the consequences of coercion or armed conflict would outweigh the potential gains. This requires the maintenance of a credible military capability and strategy with the clear political will to act."

Cyber threats to the security of the Alliance are becoming more frequent, complex and disruptive. A cyber attack on one Ally can affect all of us.

Allies have made clear that many state and non-state actors are advancing their cyber capabilities, which are low cost and growing in potency.

As the world becomes increasingly interconnected, we expect potential adversaries will rely more on cyber when seeking to gain political, military or economic advantages.

NATO Allies bear the primary responsibility for their national cyber defences. At the 2016 Warsaw Summit, Allied leaders pledged to strengthen their cyber defences as a matter of priority. NATO is supporting its Allies in this effort.

NATO protects its own IT networks 24 hours a day from cyber-attacks. We have a NATO Computer Incident Response Capability, including rapid reaction cyber defence teams on 24/7 standby that can help Allies under attack.

Such teams could be deployed, if requested by an Ally, to support national efforts in a variety of areas.

In a conventional manner, deterrence works through the communication of capability and willingness. Is this concept still applicable to the cyber realm? How can cyber-capabilities be communicated without being visibly executed against the one to be deterred?

NATO has been transparent about the actions it has taken with regard to cyber defence and has clearly communicated its intent to protect its population and territory against any threat, this includes cyber threats.

> *The Alliance has made clear it has the capabilities and willingness to deter any potential aggressor and potential attacks, including those from the cyber realm*

Through our public announcements the Alliance has made clear it has the capabilities and willingness to deter any potential aggressor and potential attacks, including those from the cyber realm.

Through cyber defence, Allies have been able to disrupt the cyber networks of Daesh to reduce their ability to recruit, to fund, to communicate.

In July 2016, Allies reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations.

An updated action plan on cyber defence was endorsed by Allies in February 2017.

The policy establishes that cyber defence is part of the Alliance's core task of collective defence, confirms that international law applies in cyberspace and intensifies NATO's cooperation with industry. The top priority is the protection of the communications systems owned and operated by the Alliance.

Following the 2018 Brussels Summit, Allies also agreed to set up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure and that NATO can draw on national cyber capabilities for its missions and operations.

> *Whatever the response to a cyber-attack, NATO will continue to follow the principle of restraint. And act in accordancce with international law*

NATO's Computer Incident Response Capability (NCIRC) based at SHAPE, Mons, Belgium, also protects NATO's own networks by providing centralised and round-the-clock cyber defence support to the various NATO sites.

Official announcements underline the necessity of NATO's partnership with industry and academia concerning cyber-security issues. As cyber operations need security gaps in hard- and software and the best cyber defence is to close relevant security gaps, what exactly is the industry's role in cooperation with NATO and its member states?

Our enhanced cyber policy defines ways to take forward awareness, education, training and exercise activities, and encourages further progress in various cooperation initiatives, including those with partner countries and international organisations.

We are further developing our partnership with industry and academia from all Allies to keep pace with technological advances through innovation.

The expertise of the private sector is crucial which is why NATO is strengthening its relationship with industry through the NATO Industry Cyber Partnership by information sharing, training and exercises.

This partnership relies on existing structures and includes NATO entities, national Computer Emergency Response Teams (CERTs) and NATO member countries' industry representatives.

To remain current and abreast of best cyber defence practice, NATO also conducts regular exercises; some of them open to industry partners. Cyber Coalition is NATO's flagship annual cyber defence exercise and one of the largest in the world. The exercise tests and trains cyber defenders from across the Alliance in their ability to defend NATO and national networks.

From defending against malware, through hybrid challenges involving social media, to attacks on mobile devices, the exercise has a challenging, realistic scenario that helps prepare our cyber defenders for real-life cyber challenges. Industry and academia also participate in Cyber Coalition.

Another example of exercises linked to NATO and open to Industry is one that has already taken place this year, Exercise Locked Shields 2019. It is an annual exercise organised by the NATO Cooperative Cyber Defence Centre of Excellence and was held from 8-12 April this year.

This exercise enables cyber security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making, legal and communication aspects.

Profile

Major General José Luis Triguero de la Torre *joined the Spanish Air Force Academy in 1975. During his more than 35 years' experience in major CIS and C2 systems, he participated in the specification, development, acquisition, implementation and management of systems at different levels of responsibility. He has extensive experience related to Cyber Defence. In March 2016, MGen Triguero took up the post of Director, NATO Headquarters Consultation, Command and Control Staff (NHQC3S) at NATO Headquarters. He is married and has three grown-up sons and one granddaughter.*

This year’s exercise was organised in cooperation with the Estonian Defence Forces, the Finnish Defence Forces, the United States European Command, National Security Research Institute of the Republic of Korea, Tallinn University of Technology, and substantial participation from industry representatives.

NATO sees – as you have just mentioned – cyber defence as its core task of collective defence and affirms that the invocation of Article 5 can happen in a case-by-case decision. Some people say that there is an on-going cyber war between member states and hostile powers, including state and non-state actors. So how far are we away from an Article 5 scenario?

NATO's main focus in cyber defence is to protect its own networks (including operations and missions) and enhance resilience across the Alliance.

We are of course aware that cyber is a challenge, in many ways. There is no military operation, no military conflict without a cyber dimension today.

We are also aware that cyber has been used to try to meddle in political democratic processes across the Alliance – that’s one of the reasons why we have significantly increased our cyber defences, the resilience of our cyber networks, increased awareness among Allies, why we are exercising, and why Allies have decided that cyber-attacks can trigger Article 5.

As for how far away are we from an Article 5 scenario, it would not be appropriate for me to speculate on what type of cyber-attack would trigger Article 5.

Any decision to invoke Article 5 and the Alliance’s potential response would be context dependent and based on a political decision.

The Alliance’s response could include diplomatic and economic sanctions, cyber-responses, or even conventional forces, depending on the nature and consequences of the attack.

Whatever the response, NATO will continue to follow the principle of restraint. And act in accordance with international law.

Turning to another dimension of security: Dialogue is, together with deterrence, often perceived as one of the two sides of the same medal. What opportunities to foster new dialogue does the cyberspace offer?

Dialogue is important no matter the domain. Transparency is a priority for our Alliance and our citizens deserve to know what we are doing.

Cyberspace offers many opportunities for dialogue. Through the online world, Allies can communicate with each other instantaneously, reach out to the general public, and media organisations.

NATO also supports efforts, such as at the UN and OSCE, to maintain peace and security in cyberspace and to promote stability and reduce the risk of conflict.

Dear Major General, thank you very much for the interview!

"INITIAL SUCCESSES IN CYBER DIPLOMACY ARE ALREADY VISIBLE"

Interview with ***Captain (GE Navy) Matthias Friese***

The participating States of the OSCE have adopted a number of confidence building measures concerning the realm of cyber security some years ago – in 2013 and most recently in 2016. But lately, there has been a lot of talk about cyber attacks originating in participating States of the OSCE. Not a few even talk about a cyber war. Is cyber diplomacy failing?

No! I quite understand the critical approach to the term "cyber diplomacy," because the incidents that you hear about are very problematic. Nevertheless, in my point of view they show very clearly that we need more cyber diplomacy and not that it has failed. Especially when regarding the fact that cyber attacks take place on a technical level, it is vitally important to have contacts and communication channels at the political level. These are simply offered by the OSCE. Let me point out only three of the 2013 and 2016 Confidence Building Measures (CBMs) to illustrate this more in detail. According to CBM 3, all participating States declare to hold consultations. It may sound profane, but apart from technical assessments, it is crucial to have political talks together in order not to aggravate tensions or conflicts. Therefore, the dialogue shown here is very important. Based on this, it becomes more concrete in CBM 8. Relying on this, a Cyber Point-of-Contact network has been established, and today 54 states have nominated their national cyber officials. This network provides fast state-to-state communication to respond swiftly and politically to any cyber or information and communication technology incidents affecting one or more OSCE participating States. By the way, the Federal Foreign Office is providing financial support for the further expansion of this contact point network in accordance with CBM 8.

It is vitally important to have contacts and communication channels at the political level

An important complement to the implementation of these policy consultations is behind CBM 13 (Use of Secure and Authorized Communication Channels). It intends to operate the existing OSCE Communication Network, which has long been successfully used for information exchange in conventional arms control, in the concern of cyber security. This network is physically made up of extra secured terminals for the exchange of sensitive data and information between the OSCE participating States. The Forum for Security Co-operation has agreed to co-use. Now the practical arrangement is worked out.

All in all, it can be seen that the OSCE is working on improving, deepening and implementing international cyber diplomacy, and that initial successes are already visible here.

However, the agreed-on CBMs for transparency, cooperation and stability are all voluntary and therefore legally non-binding. Is this sufficient to ensure that there will be no conflict in cyberspace that can develop into a conventional war?

I think on this point it is worth answering at some length: The OSCE is a regional security organization according to Chapter VIII of the UN Charter. Its purpose is complementary to the UN's aim to settle disputes and conflicts peacefully. For some time, the OSCE has identified so-called transnational threats, such as transnational terrorism or organized crime, and promotes dialogue and cooperation at a regional level to counter these threats. Cyber security has been added in 2012 as a newer form of transnational threats. Essentially, it is about preventing tensions or crises between states from escalating into conflict at the regional level through confidence building. This danger is very concrete in the context of cyber attacks. If a state in political tensions with another is attacked in cyberspace, the lacking or imprecise attribution of the authorship of the attack often creates an acute danger of escalation, as the attack may be prematurely blamed on that other state. This should be prevented by building confidence, transparency and communication between OSCE participating States.

As far as the question of voluntariness is concerned, one might have to say that it is the essence to a confidence-building measure that it is freely agreed by both parties. In that sense, it bears some importance that the OSCE Ministerial Council, that is concretely all 57 foreign ministers of the participating States, unanimously approved the decision of the Permanent Council 1202 on cyber CBMs and encouraged all participating States to further the practical implementation of the CBMs. This is what happened at the OSCE Ministerial Council 2016 - incidentally in Hamburg under German Presidency.

The voluntary nature is therefore not a shortcoming, but extremely important to build and to deepen trust.

Many experts doubt that effective arms control in cyberspace is even possible. It seems just too difficult to count computer worms and software vulnerabilities like tanks and rockets. How is this problem discussed in the OSCE?

Admittedly, that is quite correct and describes the problem of the cybersphere pretty well. It is all the more important to seek ways to prevent conflict in the cyberspace, and to this purpose the experience of conventional arms control can only be useful. Arms control should not only be seen as a legal framework "carved in stone" and should not only be judged by its effectiveness. Rather, it should be understood as a perpetual process in which different parties approach each other, exchange ideas, and at best ultimately cooperate. If we look at the development of classical arms control in the OSCE area, it has come about slowly. Some time ago, in the frame of the CSCE, the first step was laid in which the individual states provided transparency. Thus, the mutual exchange of data, intentions and plans has gradually created a basis of trust; sometimes also backed by a verification regime. Building on this, it was possible to negotiate and agree on concrete measures and mechanisms for arms control and even disarmament. Something similar is being attempted in cyber in the OSCE, which is a relatively new field in security policy. OSCE participating States regularly provide information on national cyber developments, e.g. new cyber strategies, legislation and activities. Even at the risk of repeating myself: on the political level it is of paramount importance to talk to each other in order to build trust and, based on that, to agree on concrete measures in the first place.

Arms control should be understood as a perpetual process in which different parties approach each other, exchange ideas, and at best ultimately cooperate

Currently, the option of state-run hackbacks is openly discussed in Germany. Can you assess whether this option is based on the “exchange of good practice” under CBM 15? Have participating States even described their experience in active cyber-defense within the OSCE?

Certainly not. Concrete (technical) security remains the responsibility and task of the individual states, which have suitable instruments and facilities – mostly in the area of interior ministries and security authorities –, which are surely internationally networked at their level. In any case, there is no joint planning or coordination or exchange on active (practical) cyber-defense in the OSCE. The CBM 15 aims to better protect the vulnerabilities of states, in particular the protection of critical infrastructures. To do this, among others the exchange of information, experience and good practice, as well as a shared understanding of the gravity of cyber incidents should help.

Two UN high-level committees will soon start working in New York. The Federal Republic of Germany will participate very actively in both

When is a legally binding cyber-weapons limitation or better prohibition contract to be expected?

Well, you are asking a bit beyond the scope of the OSCE. The lead in such a process would be with the UN. For cyber, the UN Secretary-General since 2004 has convened so-called Governmental Group of Experts (GGE) inter alia for the development of cyber norms. The last GGE even ran under German presidency. Two UN high-level committees will soon start working in New York: a GGE, consisting of 25 high-ranking cyber experts, and an open-ended working group (OEWG) to which all UN member states can contribute. The Federal Republic of Germany will participate very actively in both committees. The intention to create international standards for this new challenge can be recognized, but it is also known that this is “a thick board to drill” that will take a lot of time. What is new is that the GGE plans to get to know the experiences and work of regional security organizations at an early stage in the process. So maybe this is an OSCE contribution to the emergence of international norms. By the way, the GGE will first speak with the OSCE, the appointments have already been agreed. The OSCE’s work on confidence-building in cyberspace is internationally seen as a role-model anyway: The ASEAN Regional Forum started developing Cyber CBMS for Southeast Asia based on the OSCE’s Permanent Council Decision 1202 in 2018.

So you see, and that is my credo, international security cooperation needs time and, above all, mutual trust, as well as organizations like the OSCE. This is an important basis for a peaceful international order, whether “analogue” or digital.

Dear Captain, thank you very much for this interview!

Profile

Captain (GE Navy) Matthias Friese

Politico-military Adviser, Permanent Mission of Germany to the OSCE, i.a. responsible for cyber. Multiple assignments in the field of naval aviation, including commanding officer. Admiral Staff Officer Course. Desk Officer in the military policy department and the office of the Parliamentary State Secretary in the Ministry of Defense as well as in the planning staff of the Minister of Defense. Director of Studies at the Federal Academy for Security Policy. Deputy Commander Territorial Command Bavaria/Garrison Commander Munich. Publications on security policy, Afghanistan and navy (naval history).

ADIC – Agentur für Innovation in der Cybersicherheit / Agency for Innovation in Cybersecurity
Ursprünglich als „Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien“ gegründet.
Originally founded as "Agency for Disruptive Innovations in Cybersecurity and Key Technologies".

ARPANET – Advanced Research Projects Agency Network
Durch die US Air Force ab 1968 betriebenes dezentrales Computernetzwerk. Vorläufer des Internets.
Decentralized computer network operated by the US Air Force since 1968. Forerunner of the internet.

ASEAN – Verband südostasiatischer Nationen / Association of Southeast Asian Nations

BBK – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe / Federal Office of Civil Protection and Disaster Assistance

BSI – Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security

CERT - Computer Emergency Response Team

CyberAZ – Cyber Abwehrzentrum / Cyber Defense Center

DARPA -Organisation für Forschungsprojekte der Verteidigung; Behörde des US Verteidigungsministeriums / Defense Advanced Research Project Agency; Agency of the US Department of Defense

DoS/DDoS – Denial of Service/Distributed Denial of Service (deutsch: Verweigerung des Dienstes/ verteilte Verweigerung des Dienstes)
Nichtverfügbarkeit eines Internetdienstes, meist durch Überlastung der Datenleitung
Unavailability of an Internet service, usually due to overloading of the data line

GGE – UN-Gruppe von Regierungssachverständigen / Group of Governmental Experts

Hackback
Wörtlich „Zurückhacken“, virtueller Gegenangriff
Literally, virtual counterattack

IKT/ICT – Informations- und Kommunikationstechnologie / Information and Communications Technology

IoT – Internet der Dinge / Internet of Things

KdoCIR – Kommando Cyber- und Informationsraum / Cyber and Information Domain Service

KRITIS-Verordnung
Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz
Ordinance on the Determination of Critical Infrastructures under the BSI Act

NCDA – Nationale Cyber Verteidigungsbehörde. In Deutschland ist dies das BSI. / National Cyberdefence Authority. In Germany the BSI.

NCIRC – NATO-Reaktionsfähigkeit bei Computerereignissen / NATO Computer Incident Response Capability
Teil der NATO Communications and Information Agency zum Schutz von NATO-Netzwerkstrukturen.
Part of the NATO Communications and Information Agency for the protection of NATO's network structures.

PKGrG – Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumsgesetz) / Law on the parliamentary control of Federal intelligence service (Control Body Act)

script kiddies
Stereotyp über laienhafte, meist jugendliche Computernutzer, die ohne tiefergehende Computer- und Programmierkenntnisse, meist mittels gekaufter Scripts, in fremde Computersysteme eindringen.
Stereotype about amateur, mostly juvenile computer users, who penetrate without deep computer and programming knowledge, mostly by means of bought scripts, into foreign computer systems.

Stuxnet Worm

Hoch entwickelter Computerwurm, der im Jahre 2010 die Urananreicherungsanlagen im iranischen Natanz zerstörte.

Sophisticated computer worm that destroyed uranium enrichment facilities in Natanz, Iran, in 2010.

TCP/IP – Transmission Control Protocol/Internet Protocol

Internetprotokoll, Basis für die Netzwerkkommunikation im Internet

Basis for network communication on the Internet

VBM/CBM – Vertrauensbildende Maßnahmen / Confidence Building Measures

Zero-Day Exploit

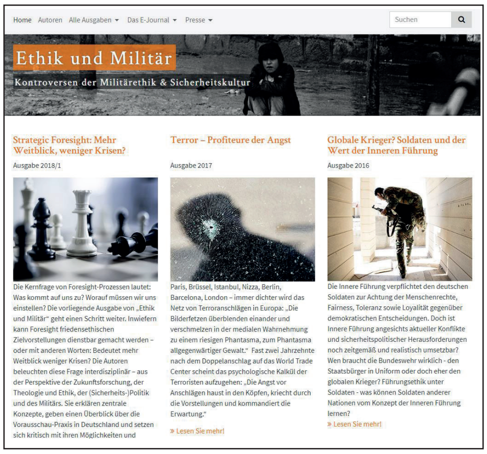
Schwachstelle in einer Computersoftware, für die noch keine Beseitigungsmöglichkeit (Patch/Softwareupdate) besteht

Vulnerability in a computer software for which a removal patch does not yet exist

ZITiS – Zentrale Stelle für Informationstechnik im Sicherheitsbereich / Central office for information technology in the security sector

PREVIEW / FULL ISSUES

www.ethicsandarmedforces.com



Strategic Foresight: Mehr Weitblick, weniger Krisen?

Ausgabe 2018/1

Die Kernfrage von Foresight-Prozessen lautet: Was kommt auf uns zu? Worauf müssen wir uns einstellen? Die vorliegende Ausgabe von „Ethik und Militär“ geht einen Schritt weiter. Inwiefern kann Foresight friedensethischen Zielvorstellungen dienstbar gemacht werden – oder mit anderen Worten: Bedeutet mehr Weitblick weniger Krisen? Die Autoren beleuchten diese Frage interdisziplinär – aus der Perspektive der Zukunftsforschung, der Theologie und Ethik, der (Sicherheits-)Politik und des Militärs. Sie erklären zentrale Konzepte, geben einen Überblick über die Vorausschau-Praxis in Deutschland und setzen sich kritisch mit ihren Möglichkeiten und

Terror – Profiteure der Angst

Ausgabe 2017

Paris, Brüssel, Istanbul, Nizza, Berlin, Barcelona, London – immer dichter wird das Netz von Terroranschlägen in Europa: „Die Bilderfetzen überblenden einander und verschmelzen in der medialen Wahrnehmung zu einem riesigen Phantasma, zum Phantasma allgegenwärtiger Gewalt.“ Fast zwei Jahrzehnte nach dem Doppelanschlag auf das World Trade Center scheint das psychologische Kalkül der Terroristen aufzugehen: „Die Angst vor Anschlägen haust in den Köpfen, kriecht durch die Vorstellungen und kommandiert die Erwartung.“

» Lesen Sie mehr!

Globale Krieger? Soldaten und der Wert der Inneren Führung

Ausgabe 2016

Die Innere Führung verpflichtet den deutschen Soldaten zur Achtung der Menschenrechte, Fairness, Toleranz sowie Loyalität gegenüber demokratischen Entscheidungen. Doch ist Innere Führung angesichts aktueller Konflikte und sicherheitspolitischer Herausforderungen noch zeitgemäß und realistisch umsetzbar? Wen braucht die Bundeswehr wirklich - den Staatsbürger in Uniform oder doch eher den globalen Krieger? Führungsethik unter Soldaten - was können Soldaten anderer Nationen vom Konzept der Inneren Führung lernen?

» Lesen Sie mehr!

This issue and all other issues of „Ethics and Armed Forces“ can be found **in German and English** on the homepage of the e-journal.

The forthcoming issue

The next issue **(available from December 2, 2019)** will be dedicated to **ethics education.**

Full issues of „Ethics and Armed Forces“

2018/2	European Army
2018/1	Strategic foresight
2017	Terror
2016	Innere Führung
2015/2	Hybrid warfare
2015/1	Military medical ethics
2014/2	Cyberwar
2014/1	Drones and LAWS

IMPRINT

The e-journal “Ethics and Armed Forces” (ISSN 2199-4137) is a free-of-charge, non-commercial, digital publication containing journalistic and editorial content.
It is produced by Zentrum für ethische Bildung in den Streitkräften – zebis, Herrengraben 4, 20459 Hamburg.
Director of zebis: Dr. Veronika Bock

Note: The published articles do not necessarily reflect the opinion of the editors and publishers.

Editors
Prof. Dr. Andreas Bock, Dr. Veronika Bock,
Prof. Dr. Thomas Elßner, Dr. Johannes Frühbauer,
Prof. Dr. Fred van Iersel, Prof. Dr. Alexander Merkl
Advisory Board
Lothar Bendel, Heinrich Dierkes, Dr. Angela Reinders,
Cornelius Sturm, Kristina Tonn
Editorial team
Jan Peter Gülden
Rüdiger Frank
Person responsible for content pursuant to section 55 (2) of the German Interstate Broadcasting Agreement (Rundfunkstaatsvertrag, RStV):
Dr. Veronika Bock, Herrengraben 4, 20459 Hamburg
Contact
Tel.: +49(0)40 - 67 08 59 - 51, Fax 67 08 59 - 3
E-Mail: redaktion@zebis.eu

Service provider as the legal entity of Zentrum für ethische Bildung in den Streitkräften – zebis
Katholische Soldatenseelsorge (KS)
Legal form
Anstalt des öffentlichen Rechts
Supervision
Catholic military bishop for the German
armed forces (Bundeswehr)
Am Weidendamm 2, 10117 Berlin
Authorized board of directors of KS
Leitender Militärdekan
Msgr. Wolfgang Schilk
Diplom-Kaufmann Wolfgang Wurmb
Am Weidendamm 2
10117 Berlin
Contakt KS
Telefon: +49(0)30 - 20 617 - 500
Telefax: +49(0)30 - 20 617 - 599
Info@Katholische-Soldatenseelsorge.de

Date of Publication: December 1, 2018

ethicsandarmedforces.com

zebis

zebis
Zentrum für ethische Bildung in den Streitkräften
Herrengraben 4
20459 Hamburg

Tel. +49 40 67 08 59 - 55
Fax +49 40 67 08 59 - 59

info@zebis.eu
www.zebis.eu