Operational Cyber – A Global View

Ralph D. Thiele

April 2013

Abstract

Access to the cyber domain has ultimately become one of the key "power sources" of prosperity. The dependence of our information society on the availability and integrity as well as on the reliability and confidentiality of data, information and knowledge makes it particularly susceptible to cyber threats. Risk management needs to strive for a balance between threats, vulnerabilities and consequences. Yet, it must no longer be performed only preventively and statically, but must rather be able to be adapted dynamically to the situation development. The dovetailing of military and civil networks constitutes a special risk for the armed forces because instabilities and failures of the common cyber infrastructure may also affect their operational readiness. The cyber domain is particularly exposed to risk especially in military conflicts due to its great vulnerability from a large distance and due to the anonymity of the attacker. However, armed forces should not only perceive the threats of this domain but also concentrate on the opportunities it provides. Modern states are completely right in acknowledging the importance of the domain of cyber. Technology moves quickly. Evolving technology is accelerating the flow of information, placing unique pressures on decision-making and action. The potential for cascading effects is amplified by the interconnectedness of cyberspace. We better prepare for a demanding new kind of challenge – in society, business and security.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is objective and task oriented and is above party politics.

In an ever more complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, bringing major opportunities but also risks, decision-makers in enterprises and politics depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, economy, international relations, and security/ defense. ISPSW network experts have worked – in some cases for decades – in executive positions and possess a wide range of experience in their respective specialist areas.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

ANALYSIS

1. Man Made

Ensuring security in the 21st century has become more challenging than ever. Global dynamics and trends keep altering developments permanently. In future, the focus of security policy will be on so-called "*global commons*" whose secured use is the basis for the security and prosperity of modern knowledge societies – unhindered access to airspace, seaways, space and cyberspace.

Cyber security is a particular complex, extremely demanding challenge. Cyberspace is difficult to grasp even conceptually. As it increasingly pervades all aspects of life, there are many, sometimes contrary perspectives and approaches. The complexity of concrete operational measures is even greater. The cyber domain enables a promising field of activity from the perspective of potential and not only military adversaries. Possible options are the effects associated with the paralyzation of certain networks such as the collapse of parts of energy supply with secondary consequences in the basic services and supplies for the population. These effects may serve, for instance, attempted blackmailing by individuals or criminal organizations and also extend to conscious acts of "*war*" of terrorist or state actors. The recent massive cyber attacks from North Korea on South Korea`s banking, media, and government information infrastructure highlight that asymmetric strikes of that kind have long become standard in difficult security situations.

Unlike other "*global commons*", cyberspace owes its development to the creative strength of humans. It is man made and provides the actors involved with largely universal access and ever more extensive options of action. This is why Kenneth Geers has pointed out that conflicts or conflict management in cyberspace are subject to special conditions.

- The Internet is an artificial environment. It can be shaped according to national/international security requirements.
- The rapid proliferation of Internet technologies makes it impossible for any organization to be familiar with all of them.
- The physical proximity of adversaries loses much of its relevance as cyber attacks are launched without regard to terrestrial geography.
- Frequent software updates and network reconfiguration change Internet geography unpredictably and without warning.
- The asymmetric nature of cyber attacks strongly favors the attacker.
- Cyber attacks are particular flexible. They can be used for propaganda, espionage, disruption of lines of communication and the destruction of critical infrastructure.
- Cyber attacks can be conducted with a high degree of anonymity which makes defense strategies such as deterrence and retaliation not credible.
- A lengthy and costly cyber war could take place without anyone but the direct participants knowing about it.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

- The intangible nature of cyberspace can make the calculation of victory, defeat, and battle damage a highly subjective undertaking.
- There are few moral inhibitions to cyber warfare.[1]

Global networking of information relationships has long become an essential basis of modern life in the overarching domain of cyber. Electronically processed data are of a great value to the government and population as valuable information is stored in each IT infrastructure: security-related data, classified information, confidential data on citizens and much more. The well-being of modern, sustainable states and societies is inseparably linked with secured and unhindered access to the virtual world.

The dualism of, on the one hand, having created the cyber domain and, on the other hand, of being subjected to an increasingly high level of dependence shows the central and irreversible importance of this symbiosis. Access to the cyber domain has ultimately become one of the key "power sources" of prosperity. Obviously national and international security provision measures will be required, starting with the protection of the personal rights of the individual up to the sustainable defense against threats to critical infrastructure, encompassing not only economic areas as the financial sector, key industries and energy supply, but also police and military. Consequently, extensive, interdepartmental and even multinational protection against attacks from this domain is rapidly gaining importance. Cyber within the context of national and international security provision is not an issue of an individual state, ministry or enterprise that contributes, for example, to the basic services and supplies but is a comprehensive challenge.

2. Definition and Threats

In mid-2010, thousands of centrifuges, enriching uranium at Iranian nuclear research facilities, run out of control though control systems reported that the centrifuges were operating normally. This incident was the work of the Stuxnet computer worm, one of the most sophisticated cyber weapons to date. The infiltration was supposed to set back Iran's suspected nuclear weapons program several years. Stuxnet was the first alleged identified instance of weaponized computer code or malware employed as a 'use of force'. Later on two other targeted computer viruses have surfaced: Duqu in September 2011, followed by Flame in May 2012. Media reports allege that both targeted Iran as well.[2] Flame also affected computers in Lebanon, the United Arab Emirates, and the West Bank. It copied text, recorded audio, and deleted files on the computers into which it hacked. New York Times chief Washington correspondent David Sanger reported in June 2012[3] that the Stuxnet cyber worm was only part of a broader operation, Olympic Games, launched against Iran by the United States and Israel. This affirmed what many suspected: Cyber attacks have become security instruments of nation states.

[1] Kenneth Geers. "Sun Tzu and Cyber War". Tallinn 2011 http://de.slideshare.net/MarioEliseo3/kenneth-geerssuntzuandcyberwar (accessed 13 March 2013)
[2] Ellen Nakashima, Greg Miller and Julie Tate. "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say". Washington Post. 19 June 2012.
[3] David E. Sanger. "Obama Order Sped Up Wave of Cyber attacks Against Iran". Washington Post. 1 June 2012.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The Verizon 2012 Data Breach Investigation Report[4] states for the year 2011 an all-time high 174 million compromised records. Primarily organized criminals continued to automate and streamline their method of high-volume, low-risk attacks against weaker targets. Less frequent, but more damaging were continued attacks against intellectual properties, particularly trade secrets and classified information. 98 % of the data breaches stemmed from external agents. 4% implicated internal employees. Activist groups stole more than 58% of all data. 81% of the breaches occurred via some form of hacking, 69% incorporated malware. 96% of attacks were not highly difficult. 97% of breaches were avoidable through simple or intermediate controls.

The dependence of our information society on the availability and integrity as well as on the reliability and confidentiality of data, information and knowledge makes it particularly susceptible to cyber threats. An aggressor nation or extremist group could gain control of critical switches and derail passenger trains, or trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across nations and regions. The most destructive scenarios involve cyber actors launching several attacks on critical infrastructure at once, in combination with a physical attack. Attackers could also seek to disable or degrade critical military systems and communications networks.

In his State of the Union address of 13 February 2013, U.S. President Barak Obama stated the issue of cyber challenge clearly:

"America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. … That's why, earlier today, I signed a new executive order that will strengthen our cyber defenses by increasing information sharing, and developing standards to protect our national security, our jobs, and our privacy."[5]

The coexistence of a variety of definitions, descriptions and interpretation attempts of "*cyberspace*" illustrates the difficulties in capturing this phenomenon.[6] The virtual information space, which is constantly growing based on networked information and communication technologies can be regarded as the lowest common denominator on a global scale. The underlying technology, in the form of networked systems, which collect, process and transmit information and data, is mostly perceived as the determinant element.[7] On careful reflection, this technology only serves as a tool and only creates the aforementioned virtual information space when combining the contents, data and information. Furthermore, the individual as a user and decision-maker must be included for the sake of a comprehensive consideration, particularly in times of highly interactive

[4] Verizon 2012 Data Breach Investigation Report. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf (accessed 14 March 2013).
[5] Barack Obama. State of the Union Address. http://www.nytimes.com/2013/02/13/us/politics/obamas-2013-state-of-the-union-address.html?_r=0&pagewanted=print (accessed 13 March 2013).
[6] Definitions and descriptions ranging from DEU Cyber Security Strategy, FMOD IT Strategy, Subconcept for Bundeswehr Command and Control Support and the Bundeswehr IT System, Subconcept for Bundeswehr Information Operations and USAF AFDD 3-12 as well as Nye jr. Joseph S., Nuclear Lessons for Cyber Security, p.19 up to CSIS - WHEN GOOD METAPHORS GO BAD: The Metaphoric "Branding" of Cyberspace
[7] Definitions of cyberspace in DEU Cyber Security Strategy and cyberspace in USAF AFDD 3-12

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

"*Web/Net 2.0*" environments, the trend towards networked-collaborative working methods and towards the "*Internet of Things*"[8], i.e. the reflection of all human communication and interaction needs and processes.

Three further important aspects need to be considered:

- the dependence on the secured supply of electricity as the basis for "*cyberspace*"
- the dependence on the unrestricted use of the electromagnetic/electro optical spectrum as a transport medium
- "*cyberspace*", as virtual information space, encompasses more than just IT systems connected via the internet.

For a comprehensive understanding of the challenges of operating in "*cyberspace*", it must be understood as an artificial socio-technological complex[9] of available and increasingly standardized information and communication technologies, accessible transmission paths and human interests. Hence, the analysis must include the IT infrastructure[10], the data and information to be processed, the principles of human organization and interaction and the resulting action patterns/processes as well as the individual user behavior. This means that understanding must go beyond the general fixation to the internet, as the basis of "*cyberspace*". Each virtual information space resulting from the networking of IT systems is to be regarded as part of "*cyberspace*" as soon as there are interfaces or connections to the outside, but not necessarily to the internet.

Consequently, virtual spaces to be considered in isolation from "*cyberspace*" are hardly conceivable today in the wake of progressive extensive networking and the associated modern demands on interoperability, mobility and flexibility. Accordingly, the following definition of cyberspace could apply:

Cyberspace encompasses on a global scale all virtual data and information spaces whose IT systems – including the data and information stored in these systems or to be transmitted between these systems – are interlinked starting from the interaction needs of users using the electromagnetic/electro optic spectrum – from permanently to at least temporarily – via the universal and public Internet up to dedicated information and communication technology interfaces.

The increase in risk in cyberspace is significantly influenced by the culture of "*hacktivism*", which is currently flourishing. The spectrum ranges from the civil society protest movement with the means available in cyberspace – e.g. from Anonymous to Anti-ACTA – up to the politically and ideologically motivated fight of contrary systems – e.g. "hacker wars" USA-China, Israel-Palestine, Pakistan-India. Loosely organized, diversely motivated and showing a broad spectrum of capabilities for cyber attacks, there is a potential that, in a concentrated manner and possibly instrumentalized through state or interest group information campaigns, may generate considerable effects using cyberspace. Not least, attention must be paid to individuals and particularly insiders because, despite the increased knowledge transfer of vulnerabilities and access routes, individual outsiders are often unable to keep up with the IT security measures of large organizations such as the armed forces.

[8] "*Internet of Things*" means progressive networking of goods of daily use such as radio and television sets, toys, kitchen equipment, automobiles etc. with internet services
9 Prof. Chris Demchak, U.S. NWC. Briefing "Thinking and Teaching Cyber Security Resilience" within the context of the modular training "Cyberspace" at the Bundeswehr Command and Staff College. Hamburg 28 March 2012.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

In spite of the shift in the threat profile for industry and large organizations from internal[11] to external threats, insiders who violate the information space in which they operate by negligence or unknowingly are responsible for the majority of security incidents in their own areas. Due to the high IT security standards in large organizations, insiders substantially contribute to the opening up of access for external attackers because this is achieved in most cases through social engineering of insiders.[12] The wide distribution and extensive private use of mobile terminals, also in the work environment and context[13], as well as the openness in using internet and online services in view of the attractiveness of the workplace have played a significant part in this development.

The difficulty lies in the assignment of the threat to an actor, both at the perception of risk and threat and at the attack itself. What kind of actors are out there? What are their motives? What opportunities would they like to exploit? What adaptations would allow them to exploit those opportunities?

Even in a conventional conflict, accompanied by attacks in cyberspace, a clear attribution of the latter and thus legal security would currently not be possible. A strategy of deterrence is therefore ineffective; risk mitigation addressed to the potential aggressor by diminishing his will to use his means or by taking his means away has little chance of success. In addition, the technological development, hand in hand with new processes and possibilities of networking as well as constraints such as far-reaching economic considerations[14] open up ever-new ways of carrying out an attack.

Scott Borg[15] has pointed out that from a business standpoint there are four kinds of cyber attacks that are possible at each stage of the supply chain:

- interrupt the operation
- corrupt the operation
- discredit the operation by undermining trust or damaging brand value
- undermine the basis for the operation via loss of control, loss of competitively important information.

A categorization of cyber security risks[16] clearly shows that, on the one hand, the full extent of damage to the security targets of availability, integrity, reliability and confidentiality is to be expected at any time, irrespective of access and motive. On the other hand, the risk fields, which can be assigned to an information space include only a few that are subject to the risk management of a user of information and communication technologies who will in future only be operational. Nevertheless, these must also be considered in a comprehensive risk assessment at operational level.

---

[10] Terminal devices, process management systems, power supply and transmission media (EM/EOS)
[11] Formerly up to 80%
[12] Verizon 2012 Data Breach Investigation Report. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf (accessed 14 March 2013).
[13] For example, communication, navigation, tactical applications such as Blue Force Tracking, http://www.wired.com/dangerroom/2010/08/iphone-app-tracks-battle-buddies-rifle-mount-optional/ (as of 13.07.2012)
[14] From COTS hardware and software, cooperation models, multinational armament projects up to savings in personnel and training.
[15] Scott Borg. Securing the Supply Chain for Electronic Equipment: A Strategy and Framework .2010. http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Securing%20the%20Supply%20Chain%20for%20Electronic%20Equipment.pdf (viewed 13 March 2013)
[16] Cebula and Young, A Taxonomy of Operational Cyber Security Risks. 2010.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Consequently those information systems need particular attention and protection which are/have

- indispensable to the functioning of the other business systems/operational systems;
- essential to those business/operational activities that create the most value for that business/its customer/operations;
- the potential to cause the greatest liabilities if they go wrong.

Cyber threats also include hardware. There is a serious danger that the supply chain for electronic components, including microchips, could be infiltrated. It is possible to alter the circuitry of the electronic components or substitute counterfeit components with altered circuitry that would contain "*malicious firmware*" and that would function in much the same way as malicious software. If the electronic components were connected to any network that attackers could access, the malicious firmware could give them control of the information systems. Even if the malicious firmware was not connected to any network accessible to the attackers, it could still contain logic bombs that could cause significant harm.

Nation states would be seriously interested in malicious firmware i.e. in installing sleeper, one-use attack tools in order to prepare defensive tools that would only be used in an extreme circumstance. They are willing to put up with very long preparation times if they can obtain capabilities that are long lasting. They are very interested in targeting hard-to access systems, such as highly protected military, intelligence, and infrastructure facilities. They might invest in dormant capabilities that would go for long periods without any interaction or operation. Finally, when larger security issues were at stake, nation states would be willing to sacrifice the profits they would otherwise be making from their part of the global supply chains. Similar arguments apply to large criminal organizations, particularly in cases where the criminals could obtain large profits by corrupting electronic equipment where there was no software to corrupt.[17]

3. Operational Risk Management

The German Defense Policy Guidelines (DPG) issued in May 2011 describe the development as follows: "*Due to its complexity, attacks* (on information infrastructures) *can also destabilize our state with serious repercussions for our national security. Given this threat from the information space, governments will need to adapt the way they see and resolve conflicts. ´Cyber attacks´ […] are developing into an asymmetric threat with serious consequences.*"[18] With regard to the established international and national network structures and the partly close links between military and civil networks – both within Germany and our partner nations and in the theatres of operation – internationally coordinated, national and thus interministerial and not least joint action is the only promising approach to achieve the aim of a secured availability and safe use of the virtual information space.

The increasing dependence on cyberspace in connection with its risk and threat development puts the "*defender*" of an information space at a major disadvantage. For this reason, risk management for the own virtual information space must no longer be performed only preventively and statically, as it is mainly presented within the context of IT security, but must be able to be adapted dynamically to the situation develop-

[17] Scott Borg. "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework". .2010.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

ment. In order to be successful in cyberspace with your own information space, the focus must be primarily on its preservation and command from within. Preservation is aimed at the availability of the information space while command is aimed at the safeguarding of the integrity, reliability and confidentiality of the data and information.

Consequently, the objectives of such operational cyber risk management should be:

1. Take precautions against immanent cyber threats to the own information space through prevention in the form of *"cyber support measures".*
2. Mitigate the effect of an attack by an adversary – with view to asymmetry and assuming that a "*hit*" can hardly be avoided – through consequence management in the form of *"cyber protection measures"* and
3. Preserve the capabilities to use the virtual information space or alternative options.

Starting points for operational risk management must therefore be sought at the determining elements of the virtual information space, i.e. the IT systems, the networking media and paths, the users and the intended use processes. The same goes for the fields of activity of technology, organization and personnel. The primary prerequisite is however a more profound risk analysis and subsequently the compilation of a comprehensive cyber situation picture, which must make it possible in the long term to move from the adverse "*reactive*" to a systematically "*proactive*" position.[19]

In view of the consistently high number of potential risks, the increasing differentiation of threatening attacks and specialization of the attackers[20] as well as the foreseeable increase in risks in the future, "[cyber security] *will become the common central challenge for the government, economy and society at the national and international levels*."[21]

Organizations of all sizes in both the public and private sectors are increasingly reliant on information and technology assets, supported by people and facility assets, to successfully execute business processes that, in turn, support the delivery of services. Failure of these assets would have a direct, negative impact on the business processes they support. This, in turn, can cascade into an inability to deliver services, which ultimately impacts the organizational mission. Given these relationships, the management of risks to these assets is a key factor in positioning the organization for success. Within the cyber security space, the risk management focus is primarily on operational risks to information and technology assets. People and facility assets are also considered to the extent that they support information and technology assets.

Operational cyber security risks are defined as operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems. This 2010 report of Cebula and Young[22]presents a taxonomy of operational cyber security risks that attempts to identify and organize the sources of operational cyber security risk into four classes:

---

18 FMOD, Defense Policy Guidelines dated 27 May 2011, p.2
[19] Radabaugh Gregory. "The Evolving Cyberspace Threat". JAPCC Journal Ed.15, p.65.
[20] BSI Annual Reports 2009 and 2011
[21] Cyber Security Strategy for Germany, p.3
[22] Cebula and Young, "A Taxonomy of Operational Cyber Security Risks". 2010.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

- actions of people – action, or lack of action, taken by people either deliberately or accidentally that impact cyber security;
- systems and technology failures – failure of hardware, software, and information systems;
- failed internal processes – problems in the internal business processes that impact the ability to implement, manage, and sustain cyber security, such as process design, execution, and control;
- external events – issues often outside the control of the organization, such as disasters, legal issues, business issues, and service provider dependencies.

The taxonomy can be used as a tool to help identify all applicable operational cyber security risks in an organization. To provide context and prioritize and manage these risks in a structured manner, it builds on a basic understanding of the relationships among assets, business processes, and services that has to be established before the risk assessment starts. Assets are the building blocks of business processes, the basic units of value in the organization, i.e. people, information, facilities, and technology. In the cyber security arena the primary focus is on operational risks to information and technology assets, although people and facility assets are also considered. Business processes are the activities that support the organization's delivery of services. Failure of these assets can have a direct, negative impact on the business processes that they support. This, in turn, cascades into an inability to deliver services and ultimately impacts the mission of the organization.

Risk management needs to strive for a balance between threats and vulnerabilities and consequences. As part of a risk management strategy, protective and sustaining controls need to be applied to assets. Protective controls help manage risk conditions, while sustaining controls help manage risk consequences.

Today, nations like the USA and Israel, Russia and China have started getting operational on cyber security. The Pentagon has been focusing its role to defend the nation in cyberspace[23] on three main tracks:

- developing new capabilities;
- putting in place the policies and organizations we need to execute our mission, and;
- building more effective cooperation with industry and international partners.

In order to develop new capabilities the U.S. Department of Defense has been investing more than $3 billion annually in cyber security to build cutting-edge capabilities in this field. The core of investment aims at training and educating skilled cyber operators to conduct operations in cyberspace. The DoD Strategy for Operating in Cyberspace[24] builds on 5 initiatives:

- Treat cyberspace as an operational domain to organize, train, and equip in order to take full advantage of cyberspace potential;
- Employ new defence operating concepts to protect own networks and systems;

[23] Remarks by Secretary Panetta on Cyber Security to the Business Executives for National Security, New York City 2012. Viewed 13 March 2013 http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (accessed 13 March 2013).
[24] DoD Strategy for Operating in Cyberspace, uly 2011. http://www.defense.gov/news/d20110714cyber.pdf (accessed 14 March 2013).

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

- Partner with other government departments and agencies and the private sector to enable whole-of-government cyber security strategies;
- Build robust relationships with allies and national/international partners to strengthen collective cyber security;
- Leverage existing capabilities through an exceptional cyber workforce and rapid technological innovation.

Through innovative efforts DoD has been enhancing ongoing cyber defence programs to hunt down malicious code before it harms U.S. systems. Over the last two years, the department has focused investments in forensics to address the problem of attribution, and obviously there are first indications for returns on these investments. Building these efforts on effective cooperation with industry and international partners gives a clear indication that national and international business and Alliances/partners of the U.S.A. will be involved soon.

4. Military aspects of Operational Cyber

The revolutionary networking options of military assets causes almost all armed forces to step up their efforts to establish complex networks for the exchange of data and information in order to keep pace with technology and thus to be adequately interoperable in the multinational context as well as to have the much needed protection and impact arithmetics for missions. The general aim of the increased use of IT is to achieve a sustainable, decisive advantage by deploying forces even more quickly, efficiently and effectively using different chains of effects that can be shaped in a flexible manner, consisting of a series of military reconnaissance, command and control and weapon elements. The information superiority obtained this way is supposed to evolve into superiority in engagement. To be able to use this engagement network continually and with the required reliability, this network is to be fully protected against interference of any kind or the resulting damage effects of successful intrusion are to be limited.

The dovetailing of military and civil networks constitutes a special risk for the armed forces because instabilities and failures of the common cyber infrastructure may also affect their operational readiness. The armed forces must continue to function also especially if in war or crisis the remaining infrastructure collapses. Even if redundancies for ensuring continuous operation are implemented in part, this dependence cannot be completely removed.

In an overarching, i.e. joint approach, which is embedded in the national context, the Bundeswehr for example tries to identify also complex risks and to assess and address their relevance adequately and comprehensively. The participation of the Bundeswehr in the National Cyber Defence Centre (NCAZ) by detaching liaison officers or officials is a logical step of interministerial cooperation, which has existed for years, for example, in the council of the IT officers of the ministries or directly at service office level with the Federal Office for Information Security. This involves weighing benefits and risks to ensure the existing core functions in each area continuously or with a calculable risk of failure. Costs always play a central role in this respect. This applies not only to companies and public administration but also to the armed forces which have long been subject to serious budgetary constraints. These lead e.g. to the development of intelligent solutions in order to save costs while maintaining operational readiness. For instance, use is made of cooperative models with industry for the

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

operation of weapon systems or of the broadband data transport capability of the internet or of civil satellite communication systems so that own autonomous but expensive IT platforms are not needed.

Thomas de Maizière, the German Federal Minister of Defence, explained in his speech on the presentation of the cornerstones of the armed forces reform on 18 May 2011: *"Security is important. I would even say that security must be given top priority. It is the primary responsibility of a country. But security must also be funded from tax revenues. This necessarily limits our ability to spend and forces us, just like Clausewitz said, to concentrate on what is essential. This has always been the case."*

The cyber domain is particularly exposed to risk especially in military conflicts due to its great vulnerability from a large distance and due to the anonymity of the attacker. It is to be assumed that in interstate, i.e. usually symmetric conflicts, attacks on the IT infrastructure are accompanied by the kinetic engagement of targets. Asymmetric conflicts or stabilization operations, however, show a picture for potential enemies which is characterized by apparently hopeless military and economic inferiority. Potential disputes and conflicts are therefore transferred to more promising fields which can certainly be found in the cyber domain due to the vulnerability of modern society. This indicates the hazard potential which arises from the use of the cyber domain from the military point of view already in peacetime, and which will multiply via crises up to war. Hence, so-called cyber defense measures are becoming increasingly important.

However, armed forces should not only perceive the threats of this domain but also concentrate on the opportunities it provides. The resulting military options through so-called Computer Network Attacks (CNA) within the scope of a cohesive, joint conduct of operations offer a vast potential of military action. The emerging possibilities and perspectives can be utilized for the purposes of the mission and the tasks of an armed force. To this end, appropriate capabilities must however be developed to use the cyber domain for own offensive military purposes within the legal context of an operation.

Military operations require above all the compilation of an enemy situation picture based on an analysis of the expected "*cyber capabilities*" of potential enemy actors as well as the knowledge of own offensive options for supporting the operations. Operating in enemy networks opens up a broad range of possibilities to achieve or prepare effects with a view to achieving own operational targets. They range from the reconnaissance of the enemy's intentions by spying out databases, the manipulation of command and control and command and control support systems to the damaging to or deactivation of key functions of computer-controlled weapon systems. The interactions between the virtual and real world and the effects that can be achieved by operations in enemy networks suggest the adoption of classical planning and synchronization procedures of military operations to integrate operations in the cyber domain like any other military asset.

Scott Borg has recently[25] developed a couple of thoughts how cyber attacks could contribute to physical attacks and vice versa, among those:

- Critical Targeting Information – Determining the target's physical location, defensive capabilities and physical vulnerabilities;
- Physical Access to the Target – Providing passage through security barriers; drawing the targets into vulnerable positions;

[25] In a Washington seminar in January 2013

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

- Cover for the Attacking Force – Blinding the adversary to what is happening or where; confusing the adversary with false information; causing diversions that would absorb the adversary's attention;
- Interference with Counter-Attacks – Causing defects in the systems or equipment for counter-attacks; interrupting activities needed respectively damaging the equipment being used to launch counter-attacks;
- Magnification of Consequences – Encouraging activities before the attack that will increase losses; interfering with efforts after the attack to limit losses; damaging systems that could substitute for those attacked;
- Parallel Attacks on the Same Targets – Hitting targets that the physical attack might miss; damaging aspects of targets unharmed by the physical attack.

Obviously there is a wide scope that can and will be explored in the future.

The unilateral renunciation of offensive military capabilities in the cyber domain has disadvantages in the fight for information superiority that cannot be compensated. Offensive cyber capabilities as non-lethal weapon systems are as a rule suitable for engaging any actor – non-state and state – and thus for establishing a certain degree of deterrence. In Germany, their use is, however, subject to strict statutory requirements: The relevant military capabilities of the Bundeswehr may only be deployed within the scope of Alliance and national defense against an armed attack or under a mandate of the United Nations authorizing the employment of the armed forces. A contribution of the Bundeswehr with own capabilities to national defense against IT attacks, irrespective of whether these can be regarded as an "armed attack" of another nation within the meaning of international law[26], is currently only possible using the constitutional provisions on administrative assistance or the employment of the Bundeswehr to prevent a particularly serious accident in accordance with Article 35 para 2 sentence 2 or para 3 of the Basic Law.

NATO has assigned cyberspace "[…] *generated by computer networks in which people and computers co-exist, and which includes all aspects of online-activity*"[27] to the four "*global commons*". The preservation of free access to these spaces and their unrestricted use are highly valued given the dependencies of the NATO countries and their partners on the aforementioned spaces and in view of globalization.[28] In the face of the global threat development[29] and the regular involvement of the organization[30] itself, NATO already included cyber protection or cyber defense in their strategic concept adopted in Lisbon in 2010. With the subsequently issued "*NATO Policy on Cyber Defence*" and the following "*Cyber Defence Action Plan*", NATO emphasizes the importance of a multinational approach to cyber defense. The three main objectives of a coordinated approach are formulated as follows: Firstly, protection of NATO networks; secondly, protection of the national networks that are connected with NATO networks or contain NATO-relevant information; and thirdly, the assurance of minimum cyber defense standards for the protection of critical infrastructure at the level of the member states.

[26] Art. 51 UN Charter
[27] Definition in accordance with "NATO Cyber Defence Concept"
[28] NATO ACT, Study "Assured Access to the Global Commons"
[29] CSIS. "Significant Cyber Incidents Since 2006". Work in progress list, Last updated May 4, 2012
[30] Spiegel-Online. "NATO kämpft gegen Flut von Cyber-Attacken" (NATO fights against a flood of cyber attacks). http://www.spiegel.de/politik/ausland/0,1518,829754,00.html (accessed of 13 March 2013).

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The two cornerstones of NATO for cyber defense are "*prevention and resilience*". Due to the asymmetric characteristics of cyber threats, in connection with the largely continued existence of identified risks and threats (persistence), but mainly due to the difficulties involved in identifying their originator (attribution), the classic military term of "*deterrence*" is replaced by "*resilience*", following the aim of "*Resilience is deterrence by denial*". Hence, action cannot be focused on a potential enemy but must be aimed at risk and consequence management within the respective sphere of responsibility to minimize one's own vulnerability. Nevertheless, the Alliance reserves all options to respond to cyber threats in case of crisis to be able to react flexibly at any time. Furthermore, cyber aspects are actively involved in NATO crisis management and are thus part of any crisis and conflict assessment.

With regard to the risk and consequence management activities carried out in advance and in parallel, the NATO Information Assurance Technical Center is centrally responsible for information security issues from an operational and conceptual perspective. In the course of operationalization, great importance is attached to the creation of situational awareness including the capabilities required to issue early warnings, conduct analyses and assessments, to the development of preferably alliance-wide standards, to the integration of cyber defense in the defense planning of the Alliance and thus in missions and exercise activities as well as to the attraction of a great deal of attention for cyber defense issues across all levels. These activities are supported by NATO's offer to assist their member states in implementing cyber defense measures. This applies, in particular, to national networks and information systems upon which NATO operations depend.

5. Implications

The dynamic developments in cyber security put the spotlight on a new era of international engagement. With the malware "Stuxnet", a new quality of intervention options in the field of networked information and communication technologies has been revealed and the discussion about cyber weapons up to the control of their proliferation has been initiated at least in expert groups. While Clausewitz believed that in warfare, the advantage rested with the defence, recent developments in cyber reverse that equation. They also unveil the enormous potential of cyber to increasing the fog of war: via furthering disruption, deception, confusion and surprise.

The use of malware by state actors has altered the realities of cyber attack. History teaches that once weapons technology becomes feasible, states deploy it. Though, in the final analysis Stuxnet is alarming not so much because of its character as concrete malware but because it proves the possibility of attacks of such quality. Stuxnet shows that creating effective malware turns on imagination, technical expertise and ingenuity. There are therefore offenders who spare no effort to attack and to sabotage, preferably unnoticed, targets which are very important from their point of view with the help of IT. While attacks on critical infrastructures and their process management systems have often been accepted as residual risk so far due to the alleged low probability, it is now important to reassess this risk."[31] Since process management systems can also be found in weapon systems, these cannot be excluded from risk assessment. Here too, attack patterns and techniques corresponding to the information flow in global cyberspace are available to interested actors for analysis and possibly development of their own capabilities.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Future cyber weapons may aim to constrain the ability of commanders/CEOs to manoeuvre, coordinate or synchronise, and to divert them from focusing on the achievement of their own objectives. Conceptually, unsettling the consciousness of an adversarial commander, or a CEO or government official, causing a loss of belief in his ability to control events and depriving him of control, helps disrupt an adversary's ability to fulfil its objectives. Destruction of an asset is one of many potential objectives that cyber weapons can achieve. Yet, to deliver code as a warhead also requires highly specific domain experience and superior intelligence capabilities that often only states possess.

While criminal entrepreneurs or state-sponsored proxies, acting at arm's length to insulate states from culpability for their policies, are emerge as a real challenges in the midterm, it seems to me that state-to-state engagement will define upcoming cyber realities. This important fact requires dedicated strategic considerations. Consequently, nations and policy makers should engage in a transparent debate over the conditions under which cyber weapons should be employed or not employed.

On an operational level an important basis for any action will be

- Secure identification and analysis of risks and threats, vulnerabilities and likely consequences as the foundations for developing courses of action.
- Operational risk management, nationally and internationally linked, which goes beyond the primarily technical IT security measures. Its core should consist of
    - active prevention, from the technology up to the users, and
    - targeted consequence management, from the preservation of the core command capability to the restoration of impaired systems and capabilities.
- Compilation of a "situation picture", which also reflects the
    - expected capabilities of potential enemy actors as well as the
    - identification and development of own offensive CNO options for supporting missions. Offensive CNO capabilities are indispensable for improving the effectiveness of own preventive and defense measures. This also benefits national security provision, possibly also at a multinational level.

Modern states are completely right in acknowledging the importance of the domain of cyber. Technology moves quickly. Evolving technology is accelerating the flow of information, placing unique pressures on decision-making and first responders. The potential for cascading effects is amplified by the interconnectedness of cyberspace. We better prepare for a demanding new kind of challenge – in society, business and security – through, and these are my recommendations, the development of

- a multinational strategic approach towards the domain of cyber
- national and multinational operational concepts for societal, business and security related cyber security.

[31] BSI (Federal Office for Information Security) Situation Report 2011. p.29.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Remarks: Opinions expressed in this contribution are those of the author.

This paper has been presented at the 3rd RINSA-KAS Joint International Conference *The Leadership Changes and Security Challenges in Asia-Pacific: European and Asian Perspectives* on April 11, 2013 in Seoul, South Korea.

About the Author of this Issue

Ralph D. Thiele is Chairman of the Political-Military Society (pmg), Berlin, Germany and CEO at StatByrd Consulting. In 40 years of politico-military service, Colonel (ret.) Thiele has gained broad political, technological, academic and military expertise. He has published numerous books and articles and is lecturing widely in Europe, Asia (Beijing, Seoul, Tokyo, and Ulaanbaatar) in the U.S. and Brazil on current security affairs, cyber security, border security, maritime domain security, protection of critical infrastructure and defence.

Ralph D. Thiele

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de