Strategic Operations in the Cyber Domain and their Implications for National Cyber Security[1]

Sven Herpig[2]

Abstract: With the public discussion mainly revolving around deterrence (either by denial or by punishment), there are actually a number of strategies which can be applied to cyber operations. A cyber strategy can be thought of as an umbrella for various individual cyber operations with the ultimate aim to achieve a strategic and / or political goal. Thus, cyber strategies can be defined as the development and employment of cyber operations, integrated and coordinated with other operational domains and forms of information warfare, to achieve or support the achievement of political objectives. Five of those strategies currently exist: going dark, deterrence, sub rosa, shashou jian, and cyber war. The implications of their existence and use create the need for proactive cyber security.

Keywords: Cyber Security, Cyber Operations, Cyber Strategies, Cyber Warfare, Deterrence, Cyber War

1 Introduction

Over the last centuries, the world saw economically interwoven countries and a tendency to lower the use of force moving towards veiled warfare. It is one of the few tools which can be used to conduct actions against an adversary without necessarily sparking chaos in the international arena. Indeed, it seems that cyber operations are currently en vogue. The cyber campaign Olympic Games, commonly referred to only as Stuxnet and its relatives, is the poster-boy of the development. Various cyber weapons were developed to work together in order to infiltrate, analyse, sabotage and ultimately erase their traces [BPBF12][Gb12][FMC10]. Olympic Games hit Iran's centre of nuclear activity, a research and production facility which otherwise could have only been affected by a physical attack (e.g. a precise air strike). The latter would have caused the death of many people and might have destabilized this region even further.

Even though Robinson, Jones and Janicke [Rm15] researched and listed a comprehensive list of current research challenges for cyber warfare, they did not include cyber strategies as one of them. With the public discussion mainly revolving around deterrence (either by denial or by punishment), there are actually a number of strategies which can be applied to cyber operations. Knowing the various options is vital because

[1] Edited and abbreviated excerpt based on the PhD thesis 'Anti-War and the Cyber Triangle: Strategic Implications of Cyber Operations and Security for the State' submitted to the University of Hull by Sven Herpig in 2014. Currently pending for final approval.

[2] Bundesamt für Sicherheit in der Informationstechnik, Godesberger Alle 185-189, 53175, Bonn, sven.herpig@bsi.bund.de

'[a] grand strategic vision of cyberspace can assist states in navigating the informational turbulence in which contemporary international politics appears to find itself. [...] Cyberspace has its myriad of problems, but a true strategic sensibility demands that long-term interests prevail over short-term opportunism' [BS11]. A cyber strategy can be thought of as an umbrella for various individual cyber operations with the ultimate aim to achieve a strategic and / or political goal. Kuehl identifies a cyber strategy as 'the development and employment of strategic capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power in support of national security strategy' [Kd09]. Starr sees it as 'the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power' [Ss06]. Thus, cyber strategies can be defined as 'the development and employment of cyber operations, integrated and coordinated with other operational domains and forms of information warfare, to achieve or support the achievement of political objectives. Cyber operations refer to the targeted use and hack of digital code by any individual, group, organization or state using digital networks and connected devices, which is directed against critical national, military or civilian information infrastructure in order to alter, destroy, disrupt or deny functionality with the ultimate aim to weaken and/ or harm the targeted political unit' [Hs15].

Thus, a comprehensive cyber strategy consists inter alia of a certain implementation of cyber security as well as all the cyber operations carried out under its umbrella, connecting them to achieve a particular political or strategic goal. Discussions about the general idea of cyber strategies started with Libicki's works on deterrence and have been developed ever since [Lm09a][Lm09b] but also go far beyond that. This paper identifies and discusses the five existing cyber strategies on a macro level and analyses their implications with focus on national cyber security. The discussion is based on the academic examination of 50 cyber operations from the perspective of strategic studies and a case study of the *Olympic Games* campaign (empirical contribution) as well as extensive research on the subject matter (theoretical contribution) including more than 300 sources on strategy, cyber warfare and related areas [Hs15]. It shall therefore provide a strategic umbrella for bridging the gap between the more technical nature of cyber operations and policy-maker understanding of their implications.

2 Cyber Strategies

2.1 Going Dark

This strategy is an extended and broader implementation of the security mechanism of air-gaping networks. Going Dark means that all systems and networks which are part of the (critical) national information infrastructure of a country are not connected neither to wider networks nor to the Internet. Gervais mentions this strategy, stating that: '[...] when

it comes to states, like North Korea, that are less technologically advanced, cyber reprisals have little effect. Reprisals to cyber attacks, therefore, ought to manifest themselves as physical countermeasures when necessary' [Gm11]. It can also mean that there is no such an infrastructure to speak of yet, due to the low level of development of this state. Relying on this strategy shows that the adopting state does not believe in its ability to defend its networks properly – or their vitality, therefore making them go dark completely. Implementing this strategy can be done partially – only the classified networks are air-gaped – or for the active networks and systems structure. This approach tries to deny the adversary any access to the systems and networks which hold valuable data or can lead to casualties. The delineation between going dark and deterrence by denial is the fact that going dark does not include any additional measures of protecting systems and networks, whereas deterrence by denial includes a comprehensive set of hardening activities (see 2.2). The Olympic Games campaign has been an implementation of a shashou jian strategy (compare 2.4) consisting of different operations which targeted an infrastructure which can be considered as 'gone dark' – and partially succeeded [FMC10].

2.2 Deterrence

Deterrence in the cyber domain is the most developed and analysed cyber strategy today, if not the only one that has been discussed thoroughly so far. In general, deterrence is subdivided into deterrence by denial and deterrence by punishment. Deterrence by denial is '[...] to deny an adversary the ability to achieve its military and political objectives [...]' [Gs61] whereas '[t]he goal of deterrence by punishment is to prevent aggression by threatening greater aggression in the form of painful and perhaps fatal retaliation' [Gk11].

The most important point of deterrence is its credibility [Kr09]. The adversary has to believe that the opponent's threat of retaliation is credible. If the adversary believes it, he will not attack and is therefore deterred, or as Gray put it: '[t]he deterree has to agree to be deterred, no matter how unwillingly' [Gc99]. One common misconception about cyber deterrence is to be highlighted first. Cyber operations are used as a means to deter any domain adversarial aggression. Cyber deterrence does not mean the use of any domain means to deter an adversarial cyber aggression. For example: the threat of use of nuclear weapons as retaliation for a cyber attack is not cyber deterrence but nuclear deterrence. If both stakeholders then implement cyber retaliation, it might lead to a 'mutually assured disruption' [Gk11].

Thus, deterrence in the cyber domain may need offensive and defensive capabilities to be in place at the same time to create credible deterrence. However, airtight defensive security could make up for the lack of offensive capabilities. The ultimate aim subsequently is to increase the own security. Kugler states that '[...] the potential payoff of a well-conceived cyber deterrence strategy is considerably greater security than exists today' [Kr09]. Deterrence using cyber operations can be implemented in various ways. Payne and Walton define three types of deterrence 1. deterrence as direct attack, 2.

deterrence as preventing from doing a provocative act and 3. aggression becomes unprofitable [PW02]. Kugler's suggestions are similar. He states that the three types of how deterrence in the framework of cyber operations could work are 1. deterrence by denying benefits, 2. deterrence by incentives as well as 3. deterrence by imposing costs [Kr09].

Deterrence is not an either-or decision. Strategies can all work at once, or equally fail together. Therefore, Starr suggested a concept where cyber deterrence is custom-tailored to the adversary [Ss09]. In the case of states, Starr suggests to carry out cyber espionage activities against them to be able to tailor the deterrence strategy. This conclusion can be derived from the nature of cyber armoury. If state A were able to penetrate the networks of state B, it can be assumed that malicious software has been planted, the perception is a persuasive here as actuality. Therefore, state B might be deterred from attacking A because it assumes that A can detonate those time bombs any time. In addition, A might have gained knowledge about the weapons that B has and can harden and shield its networks from likely retaliation which effectively render B's potential attacks useless. A might have even found more vulnerabilities to exploit B's networks for future endeavours. Therefore, credible cyber deterrence needs to be custom-tailored and relies on information acquired through intelligence operations.

Despite the opportunities mentioned, cyber deterrence faces several challenges and some authors therefore regard it as void [CK10][LX10]. Lewis for example states that, '[t]he fundamental assumption is that a correct interpretation by opponents will lead them to reject certain courses of action as too risky or too expensive. The problem is that potential opponents may misinterpret deterrent threats while others may be not feel threatened, and are therefore harder to deter' [Lj10]. In case of cyber deterrence against cyber attacks, the primary challenge is proper attribution, mentioned earlier this chapter, which undermines the credibility of cyber deterrence to a large degree. If an attacker cannot be properly identified, it cannot produce deterrence by punishment. Therefore cyber deterrence might fail. If an attacker can be identified it can still be an act of deception. There can be no 100% proof whether the clues leading to the possible attacker are genuine or as distraction as part of a deceiving cyber operation. Therefore, cyber deterrence would also fail as long as no perpetrator officially takes responsibility for the attack. Even then, terrorists for example might claim ownership of a cyber attack to spread terror, whereas the actual attacker does not want to make his involvement public. Hence, the lack of proper attribution is a large problem for credibility, and hence successful deterrence. Thus, in case of an attack and subsequent possible retaliation, the decision is deferred to the political level.

Another challenge is that some cyber attacks might be too small to retaliate against [Kr09] and subsequently undermine a zero tolerance policy [He10]. If a state communicates that it will retaliate against every cyber attack (zero tolerance) it is doomed to fail because of the sheer number of attacks and the lack of resources to respond to them. Having declared retaliation against every cyber attack but failing to do so, undermines a state’s credibility. The political level therefore has to set and communicate a threshold: how much damage a cyber attack has to do for a cyber

retaliation to trigger and therefore deterrence to take place. All cyber attacks below this threshold do not produce the effect of deterrence. The other option would be the implementation of a zero tolerance policy which would inadvertently fail and therefore diminish the credibility of cyber deterrence.

Cyber deterrence against cyber attacks (as well as other attacks) struggles to deal effectively with non-state stakeholders [Lm09b]. While not covered by this research, this potential challenge warrants mention. The threat of wiping an individual's computer is not credible enough to prevent him from trying to shut down the power grid of a country. This leads to the next challenge, the lack of impact in case of cyber retaliation against a state. Compared to nuclear weapons, cyber operations lack the ability for mutual assured destruction [Aj01] or 'unexpected higher- order effects' [Ss09]. If country A plans to invade country B and has a high chance of success, A would unlikely be deterred by B's potential to shut down the power grid and wipe important databases. A is more likely to be deterred, however if B could wipe-out A's capital city as a response to the invasion. Due to the nature of cyber weapons, cyber deterrence as a strategy also faces the problem that most cyber weapons are one use only [He10]. They exploit vulnerabilities and once the adversary notices, he can fix the vulnerability and therefore render the weapon useless (against him). The knowledge of this increases the threshold of retaliation for the deterrer owing to hesitancy to use up his cyber arsenal. This increases the threshold to a level that retaliation as a result from cyber deterrence always borders between escalation and impunity, [Kr09] or as Hjortdal puts it '[t]he strategy of deterrence is thus two-sided and, as such, contradictory—a balancing act is needed between hiding the maximum level of capability on the one hand, and communicating and proving that the capability exists on a sufficiently high level to deter other states on the other' [Hm11], a thin line. For further research on this issue, when taking into account a multi- stakeholder setting, cyber deterrence faces the challenge of extended cyber defense and collective cyber retaliation only to work if applied sub rosa but not publicly [Lm09a].

Sharma sees cyber deterrence as the only vital defence against cyber attacks [Sa09]. This is partly accurate. It is the only viable cyber defence strategy which can be applied across the (critical) national information infrastructure - as opposed to going dark which can only be partly applied. However, cyber deterrence is heavily restricted in what it can achieve.

2.3 Sub Rosa

Extraction and disruption operations using networks and computer system have been coined sub rosa activities by Libicki [Lm09b]. Subsequently, a sub rosa cyber strategy 'has some aspects of intelligence operations, and some aspects of special operations – although it is neither. Of note, sub rosa warfare is almost impossible to conduct with tanks, much less nuclear weapons' [Lm09b]. Sub rosa cyber strategy are covered in some works in a blurred pool of cyber operations, information warfare and intelligence operations, but not often distinctly discussed as a single and genuine strategy or

approach. It bears close resemblance with traditional sub rosa activities such as espionage or sabotage but is conducted through cyber operations. Thus, a sub rosa cyber strategy can be part of a major intelligence operation which also involves other elements such as human intelligence (HUMINT).

States are aware of this strategy, as Gervais suggests when stating that '[a]necdotal evidence suggests that cyber espionage is a familiar practice of state governments' [Gm11]. Betz and Stevens even suggest that sub rosa cyber strategy are aspiring to be the most prevalent cyber strategy, as compared with strategies with a higher level of intensity [BS11].

A sub rosa cyber strategy is only sub rosa as long as both parties agree it to be, or as Libicki phrases it: '[p]aradoxically, maintaining sub rosa warfare requires the tacit assent of the other side, and is therefore quite fragile' [Lm09b]. The reason to keep it secret is that the less the public knows, the easier it is to de-escalate the conflict [Lm09b]. If one of the stakeholders decides to end its secretive conduct, the sub rosa operations, if continued, turn into for example shashou jian strategy (see 2.4). This strategy has a higher level of intensity and therefore does not only mean to turn a covert operation overt, but also to increase the risk of escalation and subsequent retaliation. Keeping operations sub rosa through this strategy means decreasing the likelihood of entering the retaliation cycle [Lm09b]. The more intense and physical sub rosa operations are, the more likely they are to escalate. If state A shuts down state B's power grid, B is politically pressured to react – even more so if the perpetrator becomes public knowledge. The sub rosa cyber strategy is therefore a limited intensity strategy with a likelihood of the involved stakeholders being aware of the operations but deliberately keeping them covert in order to avoid decreasing political leeway.

There is a thin line between a sub rosa cyber strategy and the shashou jian cyber strategy. It is prudent however to differentiate those two strategies from one another for several reasons. Apart from the difference in indicators which are discussed in the respective categorization paragraphs, the core distinction is that the sub rosa strategy mainly refers to intelligence, not sabotage. This crucial element coincides with the covertness of a sub rosa cyber strategy as compared to a potentially overt character of shashou jian operations as acts of sabotage are more difficult to keep covert. Sub rosa, is not, however, anything new. It is covert intelligence operations carried out through the use of cyber operations. Therefore it is necessary to distinguish it from other cyber strategies, it is less necessary to do so from other intelligence operations.

From a state's perspective, it is prudent to start implementing a sub rosa strategy by actually strengthening the own cyber security approach. When engaging in offensive cyber activities, one can expect to be attacked as well – either as retaliation or just because of the assumption that certain attacks can just not be backtracked and subsequently attributed. It is vital to develop the defense at least to the level that it could withstand an attack mirroring the power and effort oneself puts into offensive cyber operations.

2.4 Shashou Jian

Shashou jian is the Chinese translation for assassin's mace, a strategy which refers to the ability of striking the enemy decisively and stealthily - making the fight fit the weapons [CK10][Nl05]. Incorporating this strategy into the cyber operations framework is based on the alleged Chinese use of shashou jian as a means to achieve its geo-strategic goals [Nl05]. The use of the term in this work might exceed the depth of shashou jian in the Chinese original meaning. It seems however useful to keep the term and extend the description as it reflects not only the use by Chinese strategists in general but also the connection of Sun Tzu's teachings to this concept. Sun Tzu describes this kind of strategy in his writings as relying on speed, stating that '[s]peed is the essence of war. Take advantage of the enemy's unpreparedness, travel by unexpected routes and strike him where he has taken no precautions' [SG63]. In conventional terms, an assassin's mace strategy can be pictured as an attacker coming out from cover to deal a swift blow to the victim – and at once disappears.

Libicki discusses three key roles which a cyber attack might play: '[i]t might cripple adversary capabilities quickly, if the adversary is caught by surprise. It can be used as a rapier in limited situations, thereby affording a temporary but potentially decisive military advantage. It can also inhibit the adversary from using its system confidently' [Lm09a]. All the three roles are goals that can be achieved with a shashou jian cyber strategy. It aims at the decisive points [Ja68] or centres of gravity [Rg01] of the enemy to carry out a precise blow, ignoring the rules of conduct [Fj08] to achieve a coup de grâce [Tm67]. One targeted blow against parts of the (critical) national information infrastructure that brings about a huge impact (for example bringing down the state's entire power grid).

Shashou jian is very versatile can be carried out in the framework of warfare or under the umbrella of intelligence operations. When linked to the latter, it is most likely affiliated with sabotage rather than espionage activities. Shashou jian does not necessarily work in supplement to other forms of warfare or intelligence operations, but can be a standalone strategy. Hence, sub rosa and shashou jian are not only cyber strategies, but can also be conducted under the umbrella of intelligence operations. Even if to distinguish between espionage and sabotage activities seems arbitrary, it is not. The genuine difference between sub rosa and shashou jian strategies is that shashou jian still works as an overt operation after it has successfully been carried out stealthily.

2.5 Cyber War

Schneier analyses the strategy of cyber war appropriately, '[a]nd for there to be a cyberwar, there first needs to be a war' [Sb09]. Libicki phrased it similarly arguing that, '[o]perational cyberwar consists of wartime cyber attacks against military targets and military-related civilian targets' [Ml09a]. One of the options for cyber operations is to supplement conventional warfare [CK10] the research refers to this strategy as cyber war. The often hyped 'First Cyberwar' against Estonia was merely a precursor to fully-

fledged cyber war; conducted with low technology means and without any formal declaration of war [Cm07]. At the same time, there were no conventional forms of warfare which those attacks supplemented. If a state of war had been acknowledged by either one or both of the participating states, the operations could have been described as being embedded in a cyber war strategy.

The intensity and objectives with which cyber war can supplement conventional warfare varies. Lonsdale mentioned the ability of cyber warfare to substitute tactical bombing [Ld04]. In general, the intensity of cyber operations during a cyber war is not limited. As Libicki puts it: 'once something is called war, a victim's responsibility for the consequences of its acts dissipates' [Lm96]. Compared to the other kinds of cyber operations, escalation plays a minor role, given that war is already underway. The war can still turn from conventional and cyber weapons to using nuclear weapons (an escalation) but the probability that cyber operations contribute to this escalation rather than conventional warfare is comparatively low. A state would probably more be worried and prone to escalate as response to armies invading its territory and killing its citizens and armies than about the loss of electricity in the capital for example.

The difference between shashou jian and cyber war is not only the setting (cyber war can only take place during war). In addition, cyber war does not necessarily strike stealthily or at decisive points. A cyber war operation could, for example, aim to use distributed denial-of-service attacks to deny the whole country Internet access. It could also utilize destructive viruses to destroy as much data and information within the adversary's state (including private computers, companies etc.) as possible. These broad, destructive and overt operations could be part of a coercing cyber war strategy. They would not fall within a shashou jian framework.

3 Conclusion

The analysis of possible cyber strategies shows that there is a certain cyber strategy for every occasion. In times like this, when the number of stakeholders participating in international cyber conflicts is constantly increasing and no end of hostilities seems likely, it is vital to step up the corresponding security measures, in this case: cyber security.

In terms of strategies, deterrence by denial strategy would be well-chosen to focus on securing the state's 'cyber borders'. This would mean a strong focus, policy- and resource-wise, on enhancing information security – hardening systems, monitoring networks, creating public-private cooperation, research and development e. g. of advanced persistent and volatile threats, sharing information about attacks and raising public awareness. If states wish to engage in offensive cyber strategies, it is even more important to secure the own (critical) national information infrastructure in order to deal with possible retaliation. Thus, improving cyber defenses should always come first.

Cyber security which aims at securing the nation's (critical) information infrastructure

has to take a proactive approach. One way of doing so is to focus research on traps, the so-called honeypots and honeynets – either in a virtual / sandbox environment or as raw steel version. Their research, development and deployment allow the analysis of attack vectors and behaviours, therefore allowing an adaptation of the defensive measures in order to counter future attacks following those patterns. Finding and sharing information about zero-day exploits before their use allows its correction before harm is done. In order to implement a holistic and sustainable cyber security paradigm, knowledge about offensive capabilities is crucial. In cyber security, being seconds too late can already make the difference between having an effective security in place and having none at all.

4 Bibliography

[Aj01] Adams, J.: Virtual Defense. Foreign Affairs 80/3, S. 98-112, 2001.

[BPBF12] Boldizsár, B.; Pék, G.; Buttyán, L.; Félegyházi, M.: The Cousins of Stuxnet: Duqu, Flame, and Gauss, Future Internet 4/6, S. 971-1003, 2012.

[BS11] Betz, D.J.; Stevens, T.: Cyberspace and the State: Toward a Strategy for Cyber-power, The International Institute for Strategic Studies, Routledge, New York, 2011.

[CK10] Clarke, R. A.; Knake, R. K.: Cyber War. The Next Threat To National Security And What To Do About It, Harper-Collings Publisher,^New York, 2010.

[Cm07] Cavelty, M. D.: Critical information infrastructure: vulnerabilities, threats and responses, disarmament forum, ICTs and International Security 3, S. 15-22, 2007.

[Fj08] Fritz, J.: How China will use Cyber Warfare To Leapfrog In Military Competitiveness, Culture Mandala 8/1, S. 28-80, 2008.

[FMC10] Falliere, N.; Murchu, L.O.; Chien, E.: W32.Stuxnet Dossier, Symantec Security Response, Version 1.3, 2010.

[Gb12] Graumann, B.: Cyber-security: The vexed question of global rules, Secure & Defence Agenda, Brussels, 2012.

[Gc99] Gray, C. S.: Modern Strategy, Oxford University Press, Oxford, 1999.

[Gk11] Geers, K.: Strategic Cyber Security, NATO Cooperative Cyber Defence Centre of Excellence, Talinn, 2011.

[Gm11] Gervais, M.: Cyber Attacks and the Laws of War, http://ssrn.com/abstract=1939615, Stand: 15.06.2015.

[Gs61] Snyder, G.: Deterrence and Defense: Toward a Theory of National Security, Princeton University Press, Princeton, 1961.

[He10] Habiger, E. E.: Cyberwarfare and Cyberterrorism: The Need For A New U.S. Strategic Approach, The Cyber Secure Institute, Provoking Cybersecurity Change White Paper Series, White Paper, 2010.

[Hm11] Hjortdal, M.: China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence, Journal of Strategic Security 4/2, S. 1-24, 2011.

[Hs15] Herpig, S.: Anti-War and the Cyber Triangle: Strategic Implications of Cyber Operations and Security for the State, Thesis submitted to the University of Hull for the Degree of Philosophy Doctor (PhD), 2015.

[Ja68] Jomini, A.-H.: The Art of War, J. B. Lippincott & Co., Philadelphia, 1868.

[Ka94] Krepinevich, A .F.: Cavalry to Computer: the Pattern of Military Revolutions, Foreign Affairs 30/13, 1994.

[Kd09] Kuehl, D.T.: From Cyberspace to Cyberpower: Defining the Problem. In (Kramer, F.D.; Starr, S.H.; Wentz, L.K. Hrsg.): Cyberpower and National Security, National Defense University, Washington D.C., S. 24-42, 2009.

[Kf83] Kaplan, F. M.: The Wizards of Armageddon, Simon and Schuster, New York, 1983.

[Kr09] Kugler, R. L.: Deterrence of Cyber Attacks. In (Kramer, F. D.; Starr, S. H.; Wentz, L. K. Hrsg.): Cyberpower and National Security, National Defense University, Washington D. C., S. 309-342, 2009.

[Ld04] Lonsdale, D.: The Nature of War in the Information Age. A Clausewitzian Future, Frank Cass, London, 2004.

[Lj10] Lewis, J. A.: Cross-Domain Deterrence and Credible Threats, Center for Strategic & International Studies, 2010.

[Lm96] Libicki, M. C.: Protecting the United States in Cyberspace. In (Campen, A. D.; Dearth, D. H.; Goodden, T. R. Hrsg.): Cyberwar: Security, Strategy, And Conflict In The Information Age, AFCEA International Press Fairfax, Virginia, S. 91-105, 1996.

[Lm09a] Libicki, M. C.: Cyberdeterrence and Cyberwar, RAND Project AIRFORCE, RAND Corporation, Santa Monica, 2009.

[Lm09b] Libicki, M. C.: Sub Rosa Cyber War. In (Czosseck, C.; Geers, K. Hrsg.): The Virtual Battlefield. Perspectives on Cyber-Warfare 34, IOS Press, Amsterdam, 2009.

[LX10] Lan, T.; Xin, Z., Can Cyber Deterrence Work? In (Nagorski, A. Hrsg.): Global Cyber Deterrence. Views from China, the U.S., Russia, India, and Norway, EastWest Institute, New York, S. 1-3, 2010.

[Nl05] Navrozov, L.: Chinese Geostrategy: 'Assassin's Mace', http://archive.newsmax.com/archives/articles/2005/10/20/172811.shtml, Stand: 21.05.2015.

[PW02] Payne, K. B.; Walton, D. C.: Deterrence in Post Cold-War World. In (Baylis, J.; Wirtz, J.; Cohen, E.; Gray, C. S. Hrsg.): Strategy in the Contemporary World, Oxford University Press, New York, S. 161-182, 2002.

[Rg01] Rattray, G.: Strategic Warfare in Cyberspace, The MIT Press, Cambridge, 2001.

[Rm15] Robinson, M.; Jones, K.; Janicke, H.: Cyber warfare: Issues and challenges, Computers & Security 49, Elsevier, S. 70-94, 2015.

[Sb09] Schneier, B.: So-called Cyberattack Was Overblown, http://www.schneier.com/essay-280.html, Stand 20.04.2011.

[Sa09] Sharma, A.: Cyber Wars: A Paradigm Shift from Means to Ends. In (Czosseck, C.; Geers, K. Hrsg.): The Virtual Battlefield: Perspectives on Cyber-Warfare 34, IOS

Press, Amsterdam, S. 3-17, 2009.

[SG63] Sunzi; Griffith, S. B.: The Art of War, Oxford University Press, Oxford, 1963.

[Ss06] Starr, S. H.: Towards an Evolving Theory of Cyberpower. In (Czosseck, C.; Geers, K. Hrsg.): The Virtual Battlefield: Perspectives on Cyber-Warfare 34, IOS Press, Amsterdam, S. 18-52, 2009.

[Tm67] Tse-Tung, M.: Selected Military Writings of Mao Tse-Tung, Foreign Language Press, Peking, 1967.

[Wi07] Winkler, I.: Zen and the Art of Information Security, Syngress, Rockland, 2007.