Super-empowering of Non-State Actors in Cyberspace

Nikola Schmidt
nikola.schmidt@fsv.cuni.cz

PhD candidate
Department of International Relations, Institute of Political Studies
Faculty of Social Sciences, Charles University
Prague, Czech Republic

Draft – please do not quote or circulate without author´s permission

Abstract

The concept of non-state actors and their ability and power to push through their interests has been studied especially since 9/11. In the meantime, we have been witnessing a growing dependence of our society on cyber related infrastructure what has triggered a debate about all cyber-related threats. This trend has been visible in any newly adopted strategy of national security, where cyber is treated as one of the most problematic threat of present techno-centric societies. However, most of the strategies are defense-oriented and tend to focus on empowering core and wide capabilities of a nation state to secure national cyberspace. This paper asserts that cyberspace is a domain in which offense dominates the defense and where critical knowledge is more important for success than powerful forces. Additionally, given the fluid nature of cyberspace, threats are fluid as well; espionage has never been more effective, centralization has become a dominant design for critical infrastructures and critical knowledge is more important than a strong conventional army. That said, the paper fundamentally argues that all these characteristics raise the potential of so-called super-empowered non-state actors. This diffusion of state power is shadowed by a curtain of argumentation that strong defenses would avert state-sponsored attacks. This contribution to the debate attempts to emphasize that the strategic threat lies predominantly in these super-empowered individuals, and conceptualizes the dynamics of their emergence and activity.

Introduction

In the first part, the paper proposes a brief reconceptualization of some concepts such as war, state sovereignty and space, territory, cyberspace. Among those concepts, new means of power that apply in cyberspace – a critical knowledge and a power to influence so-called general knowledge – are discussed. In the middle part, the paper briefly analyses offense-defense theory, how it applies in cyberspace, and argues why offense tends to dominate defense in the cyberspace and what does a claim "super-empowering of non-state actor" means. Here, the paper argues why states would tend to behave as non-state actors rather than responsible states as they are certainly going to exploit the attribution problem to their advantage. Hence, in the end the article proposes several arguments why such super-empowering would contribute to the offense domination and proposes an empirical evidence in policy making that states already favor an offensive approach even though it is called a defensive one.

1. Concepts that need to be reconceptualized

This article does not have an ambition to fully explore following dilemmas; its objective is rather to show that a new way of strategic thinking in cyber security research would be appropriate and that a wide spectrum of conventional security concepts cannot be easily and directly applied as many authors of cyber security related literature actually tdo.

1.1. War

The core objective of this part is to read specifically Clausewitzian thoughts on war[1] and their application to a cyber conflict and to develop an argumentation why we should not hesitate to call a particular conflict in cyberspace a war. On the one hand, the reflection supposes to be critical enough to avert possible blur by securitization discourse that undermines appropriate evaluation of threats emanating from cyberspace. On the other hand, I argue that if the on-going events fulfill certain characteristics and criteria, it should be called a war even though the situation does not lead into the madness of conventional war full of bloody violence. Criteria matter in evaluating the conflict and making a decision whether it is a war or not,[2] but criteria need to be re-evaluated and reconsidered in time if the origin, means, method, progress and shape of the conflict changes; the war changes as well. An important reason to call some activity a "war" is to put certain attention to a certain conflict and, of course, to apply and to explain appropriately international law to mediate it or to vindicate a counter action – self-defense in an active way.[3] Securitization processes[4] serve here as an alarm and should be critically analyzed, not refused. Critical perspective properly warns about bending the reality by securitization discourses. Impacts of these securitization processes have been studied in the cyber security

[1] (Clausewitz et al. 2007)

[2] On of the most systematic work on war in the 20th century was undergone at the Chicago University in 40s by (Wright 1983)

[3] Article 51 of UN Charter.

[4] (Buzan, Wæver, and de Wilde 1998)

research[5] and the whole critical perspective on the birth of the concept of cyber war as well.[6] Miriam Dunn Cavelty has conducted work where she divided the securitization discourse into three branches: criminal, technical and military.[7] This paper would be situated into the third, military discourse. However, I argue that we can recognize an opposite discourse trying to undermine any kind of warnings in the name of critical thinking.[8] Some of these warnings may materialize into serious devastation or disturbance of a country just because of *clausewitzian policy continuation* of other countries or because of any conceivable objectives of non-state actors without sparing a drop of blood. Seriousness of a conflict and its alteration into a war is not measurable only by lethality of course, as will be argued, and lack of lethality should not be an argument to resist naming a cyber conflict a war. The point here is to have an appropriate policy set-out to act ably if certain cyber conflict escalates significantly. The threshold of the escalation is a critical problem.

War is usually understood as a large-scale, long-lasting, organized military and violent conflict.[9] However, war is a broad academic subject of study,[10] hence to provide a sufficient definition is much more about history-long debate rather then a precise definitional sentence. The analysis has to be anchored somewhere and for this purpose I will draw primarily on Carl von Clausewitz's classical piece *On War* and Thomas Rid's article *Cyber War Will Not Take Place*[11] which uses Clausewitz's perspective to argue that what is going on in cyberspace is definitely not a war. My core argumentation lies on a presumption that any (future) conflict, in which state A is willing to continue its policy despite widely accepted rules of international society, does not need to be bloody but it will still fulfill strategic military objectives of that state that may significantly support an operation aimed to undermine, or march contrary to, the policy of state B on its territory or where B is supposed to be the sovereign – over national cyber installations, a critical infrastructure or in the general meaning of its democratic constitutional foundation. If these foundations or sovereign interests of a particular state is disturbed or significantly influenced despite the will of the respected state and the activity can be understood as being outside of any internationally accepted norms we should consider such behavior as an *intervention*, and if it is significantly deteriorating sovereignty of the respected state for a long time and international society understands such behavior as completely unacceptable in the perspective of no intervention clause, it should be called a *war* and approached appropriately. The question is of course again, where is the threshold?

[5] (Cavelty 2008)

[6] (Kaiser 2015)

[7] (Cavelty 2012)

[8] (Gartzke 2013)

[9] Some thoughts on war related to this article would be additionally found in (Krause 2009) However, the most important study and its current reflections in cybersecurity comes from (Clausewitz et al. 2007)

[10] One of the most elaborate study about war in the 20th Century is (Wright 1983).

[11] (Rid 2012)

Classical thinker Carl von Clausewitz described war as an *"act of violence to compel our opponent to fulfil our will"*[12] where he points to the physical force as a means to compel our opponent. However, in another part of his book Clausewitz defines war as *"a continuation of policy with other means"*[13] where "means" does not necessarily include violence; it includes force that might be violent. The utmost version of violent force should be considered a thermonuclear war, however, as Russian physicist Sakharov mentioned, such a war would not be a continuation of policy with other means but rather means of universal suicide.[14] Nevertheless, even such a suicide is still called a war. In a cyber war, the violence could be completely avoided, but it does not mean that such *war* lacks its strategic military objectives and cannot be conducted as a main campaign instead of a mere support to a conventional operation.

Thomas Rid argues in his article that war according to Clausewitz should be instrumental, violent and should have political nature, while cyber war lacks all these characteristics.[15] Rid found in Clausewitz's work a request for instrumentality, which is not – by Rid's words – present in cyber war. Instrumentality means that the attacker has an objective and is reaching it by whatever means available, preferably by violent force as a means of a military strategy. A debate over instrumentality in nuclear weapons is quite broad in the core strategic literature;[16] however, drawing on Sakharov we can accept total lack of instrumentality in thermonuclear war due to the suicide effect – Mutual Assured Destruction (MAD)[17] is not a rational objective. On the other hand, mere possession of nuclear weapons has had an unprecedented deterrence effect.[18] Schelling mentioned that the military strategy changed due to their existence and that the victory cannot be measured only by military conquest but rather by a *diplomacy of violence* in which *"the art of coercion, of intimidation and deterrence"* matters;[19] Schelling aptly asserts that *latent violence* can be used to an advantage and as a coercion of people and governance to achieve victory avoiding a destructive war.[20] Schelling claims that *latent violence* is a kind of power to compel our enemy – thus, holding such a power and its usage against our enemy in a coercive diplomacy is instrumental – it is a military strategy aiming to fulfill an instrumental objective – it is a prerequisite for war if not a war as such. The same applies to a cyber war.

[12] (Clausewitz et al. 2007, 44)

[13] (Clausewitz et al. 2007, 38)

[14] (Sakharov and Salisbury 1968, 36)

[15] The discussed article (Rid 2012) has a successor in a book by the same author with a same name (Rid 2013a)

[16] See the classics in the strategic thinking: (Brodie 1946; Brodie 1959; R Jervis 1989; Kahn 1960; Schelling 1966)

[17] Mutual Assured Destruction – MAD – is a term used for a complete non-instrumentality of nuclear weapons as the attacker would never reach an objective without its own destruction. For a current debate and overall literature review see for example (Lieber et al. 2006)

[18] Debate whether nuclear weapons would definitely establish peace in the world are discussed for example in (Robert Jervis 1988; Sauer 2009; Schneider 2008)

[19] (Schelling 1966, 34)

[20] (Schelling 1966, 30)

Pure Clausewitz's thoughts do not seem to bring us an appropriate argumentation whether thermonuclear war or cyber war are wars, because his thoughts do not seem to be directly applicable to all novel situations; novel predominantly in their technology advancement. However, that does not mean that novel technology driven wars are not wars as Rid tries to convince us. Those novel situations are the result of technological development, and even if such *policy continuation* is not meaningful in thermonuclear war for its insane violent results, it is still possible – if not in nuclear bombing, in nuclear deterrence for sure. In Schelling's words it is a military strategy switched to a coercive diplomacy supported by nuclear weapons – it is a kind of violence, but not lethal. Hence, it does not lose its strategic instrumental objectives. Additionally, force made by cyber means is not insane in the same way; avowedly the opposite applies with some new additions – there is no method how to measure the "cyber armament" of our enemy. However, such armament can be used as a significant addition to conventional warfare or conducting warfare itself by taking control of critical systems on which the country runs without physical force. In that case, it definitely fulfills Schelling's concept of *latent violence* and is for sure instrumental*.*

Long lasting debate has lived over lethality and violence: the second Rid's precondition – violence – to call particular conflict a war based on Clausewitz reading. Rid builds his argumentation on the assertion that war has to be both lethal and violent[21] John Stone answered[22] to Rid and pointed out that violence does not necessarily include lethality and that violence should be understood as a force against someone who has to counter it; it can be conducted against things as well; hence, lethality is not a precondition for violent behavior. The nuclear deterrence would serve as an example. However, Rid argues that there is no violence in cyberspace. It seems that he treats violence and lethality as equal or as equally important in the analysis. Stone replied to him that the common problem already identified by Hannah Arendt in strategic thought is overlapping meaning of concepts such as power, strength, force, authority and violence.[23] Additionally, Hannah Arendt mentioned that the Clausewitzian presumption of enforcing our opponent to fulfill our will (or wish) is based on *power* instead of *violence*. *"Power of a man over a man"* is the point of Clausewitz and power definitely is not enforced merely by lethal violence.[24] In that perspective, the core of Clausewitz argument is not about lethality, but violence that implies power. Lethality is derived from Clausewitzian physical power that was the only meaningful power at the time when Clausewitz wrote On War; however, a new kind of non-violent power has been emerging in the cyber space and non-lethal violence has already been present in international relations for decades. Thus why the surprise in the strategic thinking we have been experiencing during the last years.

[21] (Rid 2012, 7)

[22] (Stone 2013)

[23] (Stone 2013)

[24] Clausewitz cited from (Arendt 1972, 37)

John Stone showed that a war does not need to imply lethality,[25] but it should include violence. We already mentioned that violence and force could be seen also in coercion instead of bloody lethality only. In Rid's answer to Stone's criticism, Rid draws on political philosopher Alessandro Passerin d'Entrèves and argues that traditional violence differs from violence administered through a cyber attack in two ways: it is *direct* and *qualified*.[26] First, a cyber attack cannot cause a direct harm to a human body – it can do so only indirectly by empowering some systems, not by code itself. Second, violence has to be qualified, which in d'Entrèves words means a transformation of force into power – institutionalized power, accepted authority. A force transforms into power by institutionalization, e.g. by law or customs, while fear transforms into respect, coercion into consent, because *"force, by the very fact of being qualified, ceases to be force"* and transforms into power.[27] Hence, the law has to be enforced by *sovereign* to be institutionalized. Additionally, why the sovereign, the ultimate authority, has to be limited to a state? When states are limited in their capacity to enforce law in the cyberspace, then sovereign in cyberspace can be any non-state actor capable to lay down a new regime that others follow, or the one capable to weaponize code in its direct or indirect effect. I have to disagree with Rid's position that violence in cyberspace is unqualified as explained above. The environment is constantly and fluidly changing;[28] it means it is complex enough, but we have to find a way how to demarcate areas, territories or spaces in cyberspace where any actor can play a role of being sovereign; in spaces that changes fluidly. The transformation of force into power by enforcing law or by laying down rules or a regime by governments[29] is widely and visibly evident in such "cyberspaces" and thus such violence is definitely qualified. We have to detach ourselves in the analysis from a physical space as the only territory of serious people's interactions. Based on such explanation we can directly argue that states are not sovereign in cyberspace on a wide variety of fronts, however, cyberspace causes national security issues to the states.

Another argument is Rid's focus on a directness of violence on human body, but violence does not need to be limited to human body, as it can target a technology as well. Human body can be directly or indirectly dependent on technology (cardiac pacemaker) and in that perspective talking about directness is inappropriate as a gun shoots bullets; in that perspective human body is not inflicted by the gun, but by the bullets. As we are increasingly dependent on technology,

[25] (Stone 2013)

[26] (D'Entreves 1967) cited from (Rid 2013b)

[27] (Rid 2013b) – cited from Rid, see (Arendt 1972)

[28] Fluidity is a characteristics that I discussed here (Schmidt 2015). The term is based on a postmodern theory by Zygmunt Bauman (Bauman 2000), which discusses constantly changing norms in a postmodern society that losses its general anchors as a result. Cyberspace can be divided into layers (Libicki 2007, 8) whereas norms belongs to the fourth cognitive layer. However the cyberspace is differently fluid on each layer: first, the physical layer that constitutes the topology of the network is constantly changing and enlarging; second, the syntactic layer is the least fluid layer and consist of communication protocols – means of communication; third, the semantic is the most fluid one as the data on the web are changing extremely fast. Forth, the cognitive is about our habits that in mutually constitutive way changes the character of cyberspace.

[29] (Lewis 2010)

human body is also more vulnerable when certain technology is targeted and it does not need to be inflicted only by bullets when someone wants coerce us by new kind of power. Such example proves us that the power has already been transformed from a bloody violence, through *latent violence* into something maybe in future called cyber violence.[30] It is latent due to immeasurability of cyber armament and due to non-physical nature of cyberspace. Additionally, deliberate indirectness of a cyber attack does not relieve its responsibility under a military cyber operation as already analyzed in Tallinn Manual,[31] because international law knows a term *"chain of events"* in the context of the rule about indiscriminate means and methods that are prohibited when undergoing military cyber operation,[32] hence a need for directness can be refuted on more than one basis; even a deliberate indirect cyber attack is understood in (the interpretation of) international law as an illegal act in cyber warfare. In that perspective, a request of pure directness is not an argument to name a cyber attack as a non-violent action in all cases.

Moreover, power matters in Clausewitz, not violence, and where power matters political nature is present. Though there are some distinctions between conventional war and cyber war, it is still war and not a kind of war similar to a war against cancer; what is Rid's metaphor used for cyber war. To summarize the argumentation we should come back to Clausewitz and read it very directly. Although he wrote his masterpiece in a completely different technological environment, his "compellence of our enemy" is about power and that is what matters in war – thus we can face a cyber war without a spared drop of blood, and it will still be a war.

War is then an on-going process during which we exercise our power to compel our enemy to fulfill our will, whereas conquest is *"the subjugation and assumption of control of a place or people by military force."[33]* Conquest fulfills that instrumentality Rid requires; a victory reached by military force and cyber power can definitely be transformed into military force as argued above. In that perspective, war is violent even though it is not lethal and bloody, and conquest seems to be achieved when people are put under certain control within a particular territory using force. Military force can be completely non-lethal; e.g. disturbance of critical infrastructure or taking control of it, or during information operations (IOps) that seek to take several groups of people under a certain level of mind control during rising star in new concept called hybrid war.[34] One may raise a question what level of mind control is already violent and what level of violence is a threshold to name a conflict a war. Tallinn manual proposes two overall categories: the "scale and effects" of the particular cyber attack. Scale is about subjective seriousness, whereas effects violating law that can be considered as a use of force are certain:

[30] *Cyber bullying* is a very proper example where this new kind of power can coerce other people to fulfill interests of the attackers without bloody violence.

[31] (CCDCOE 2013)

[32] (CCDCOE 2013, rule 43, par. 5)

[33] ("Oxford Dictionary Term: 'Conquest'" 2015)

[34] (Schmidt 2014)

damage, destruction, injury or death.[35] From my perspective, those criteria are conservative, insufficient and would never address precisely the nature of cyber war; neither when cyber war focuses on critical infrastructure on which certain citizens are extremely dependent and thus can be taken "under control" by effective short-term deception, nor when it comes to a mind control by long-lasting, hidden and silent propaganda in a hybrid war.

Rid uses the term *traditional violence* and differs it from violence administered through a cyber attack. I argue that the objective of any conquest that is focused on controlling people and territories would not need to be traditionally violent and it is still a conquest – a territory under control. Controlling minds by propaganda would require deeper analysis. The traditional force has changed, but it is still violence and in the end this new force transforms into a new power. When Thomas Rid argues that a war has to be violent drawing, on Clausewitz's and Alessandro Passerin d'Entrèves's notion of violence and thus by his words "cyber war will not take place,"[36] I argue that we have to reconceptualize war if there is instrumentality, political nature and a new kind of violence indirect against human body, but qualified in transformation of force into power. This is the first important and conclusive point of this article.

We have to be able to react when one state or non-state actor attacks another through the new kind of force that is free of lethality, but is a demonstration of a new power. Hannah Arendt pointed out that war, as a final arbiter in international relations, has never been exchanged with anything else;[37] however war has certain levels of violence and lethality is just the most visible part on the top of it.

1.2. State sovereignty, territory, space and cyberspace

State sovereignty gives the right to a state to exercise its jurisdiction over its territory, but also over a cyberspace generated by physical systems situated on that territory as explained in Tallinn Manual.[38] Does it mean that Tallinn Manual grants cyberspace a territory by addressing particular rights of states in international law? If so, then influencing such a territory should be understood as a violation of state's integrity and thus sovereignty.[39] According to the Tallinn Manual, international experts (the authors of the manual) did not reach consensus whether other than physical intervention causing physical damage would violate state sovereignty.[40] What physical intervention we may expect in a virtual space of cyberspace? Probably only an indirect, but this point still waits for analysis; however, if a cyber attack is apparently part of a wider military operation such as the one conducted by Israel against Syria in

[35] (CCDCOE 2013, rule 11) The criteria are quite more complex and can be found in cited rule.

[36] (Rid 2012)

[37] (Arendt 1972, 5)

[38] (CCDCOE 2013, rule 1, par. 5)

[39] Sovereignty as the term itself has developed during the centuries. Its meaning here is prevalently about the right of a state to exercise jurisdiction over its territory even though the territory in cyberspace seems to be blurred. For more reading about sovereignty see (Bartelson 1995)

[40] (CCDCOE 2013 Section 1, rule 1, paragraph 6)

2007, it is understood as a part of a military operation (an airstrike) and the international law applies. The cyber attack helped to physically destroy an alleged nuclear reactor with an airstrike by blinding the radar system of the Syrian army. The disputable point here is whether a pure cyberspace attack on cyber installations such as critical infrastructure or direct influencing citizens and decision-makers is a violation of state sovereignty. Can such operation be approached as a violation of territorial integrity? Experts have no consensus and I argue yes, it should be based on the argumentation above; however, a state practice is what creates customary law and the current perspective will highly probably change with the time as non-violent cyber or hybrid warfare is a great opportunity how to circumvent international law as Russia has shown us in recent years in a row of examples.[41]

If current international law is not able to stop certain activity undermining sovereignty and at the same time international society fails to call that activity a war or violation of sovereignty we have to reconsider criteria of war and more precisely analyze sovereignty in cyberspace. Another concepts that should be reconceptualized are meaning of territory and space in cyberspace. Is cyberspace a space and thus a sovereign territory when the word “cyber” has a suffix “space”? Advancing military operation by cyber means does not need to be limited to cyber attacks on radar systems as in the case of Syria 2007. First, already mentioned information operations (IOps) would influence particular citizens’ admissibility of particular territory annexation in networks outside the physical territory.[42] Its difference to mentioned Syria cyber attack 2007 is because IOps are completely separated from physical activity. If such operation were focused to influence minds of citizens, it would be approached as a violation of state’s sovereignty of the attacked state, because it addresses (attacks) people on a particular territory. If the military strategy is to annex a territory, IOps can be a prerequisite to conquest it. In that perspective and in such consequences, cyberspace should be understood as a territory albeit topologically different to a physical space, but still a sovereign territory or space where a particular state should be a sovereign. Second, the same should apply to any pure cyber attack against information systems to disrupt them in a sabotage operation. However, if a non-state actor conducts the attack, it will be considered an act of crime or terrorism, but definitely not a violation of international law even though it has an impact on the whole state. This moment gives windows of opportunity to non-state actors as an entity, however, in the end it can be conducted stealthily by states and we are witnessing, or at least we suspect, states of doing so. States tend to play a role of non-state actors by exploiting the problem of attribution in cyberspace, which gives them an opportunity to use a cyber attack to achieve their objectives in the territory of other states and to circumvent international law. States thus have so called dual-interest in establishing more repressive regime with better control over the Internet or more precise definition of state’s

[41] For more thoughts about state’s sovereignty in cyberspace and its current debate see (Lewis 2010; Herrera 2006; Franzese 2009; Cox 2002; Deibert 2009). For more thoughts about how Russia conduct its disputable hybrid war see (Pomerantsev and Weiss 2014; McDermott 2014)

[42] (Scaparrotti 2012; Waltz 1998; Blank 2008)

sovereignty in cyberspace. Such situation empowered by attribution problem in cyberspace (problem that majority of attacks cannot be attributed with particular certainty to a state) can lead to escalation of conflict and to conventional war. Let's have this point of states' dual interest as the second important conclusion of this article.

The common criticism of the above argumentation is that we cannot put equal sign between opportunity and threat[43] in cyberspace; however, having an opportunity that is compatible with possible military strategy of our enemy is a threat. Such criticism usually rises from conviction that territories are not annexed in the 21st century; however, Russia annexed Crimea without hesitation and continue to do so elsewhere on Ukrainian territory. Systems running critical infrastructure are full of vulnerabilities that may be exploited. Even after years of Stuxnet attack the same systems were still unpatched and vulnerable in other nuclear facilities and in Natanz as well.[44] This hacker's opportunity is a serious threat to national security of any developed country; hence drawing doom scenarios is not a completely insane and senseless approach of policy making.

1.3. Means of power

Each space for operation is approached as a domain in military doctrines; cyberspace as well.[45] However, drawing lines as borders in cyberspace is unreachable from the technological point and the mentioned conservative method used in Tallinn Manual is on a long-term basis untenable. Services, servers, webpages etc. are interlinked and each part would lie on a different physical territory, but they work together, being mutually dependent. Cloud computing would serve as an ultimate example. However, each domain has different challenges and domination over each domain requires different technology (ships, planes etc.). Domination in cyberspace needs to be significantly different due to the fact that cyberspace is not a physical domain. Domination with physical equipment thus loses its sense. However, cyberspace can be divided into layers and domination in each layer requires different tactics and technology. Martin Libicki described what is needed to dominate (conquest) each layer.[46] Briefly said, the first layer, the physical one consists of routers, cables, switches and can be dominated by destructive physical power; the second syntactic layer can be dominated by taking control of those systems, their firmware; the third semantic layer is about data and can be dominated by censorship or controling access to information; but the fourth one, the cognitive or pragmatic layer is tough to dominate as it is about our reflexion of reality based on cyberspace.

First, information operations focusing on our cognitive perceptions would stand as a domination operation influencing our knowledge and thus capability to perceive outer reality – *influencing mind*. Second, capability to attack critical infrastructure systems (or whatever system) by having *a critical knowledge* would represent another means of power. However, those

[43] (Gartzke 2013)

[44] (Collins and McCombie 2012)

[45] (US-DoD 2011)

[46] (Libicki 2007)

"knowledges" should be analyzed and capability in each "knowledge" should be approached as means of power in cyberspace.

2. Three types of power that matter in cyber war

We drew four layers of cyberspace; however, there is a possibility of merging the third semantic and the fourth cognitive layer in one for purposes of power differentiation in each layer. Then we can differentiate powers into two categories: *physical* based and *knowledge* based. Physical power is not important for the following analysis, because the power of physical destruction of cyber assets can be conducted by traditional conventional ways and as such, it is not the point of this article. Power of knowledge is the other category of power. Two types of knowledge that significantly matter in any kind of cyber operation is, first, *mind influence* aimed to bending the overall (or general) knowledge, cognitive perspective and reflection of the outer world and, second, a *critical knowledge* that serves to conduct a successful cyber attack on specific assets on which state is dependent and thus their malfunction may influence national security.

First, mind influence of overall knowledge about the outer world is shaped by available information and our critical capability of its assessment – a cognitive capacity. The way we cognitively assess and perceive outer reality – a world, how we make opinions and make different decisions on it or relativize some facts are objectives of information operations in military environment;[47] no matter whether they are aimed to broad public or high profile decision makers. Conducting such operations is based on creating, influencing or denying specific discourses that flow as an interaction between people through social networks as never before. Such power was called by French philosopher Michel Foucault *discourse as a power*.[48] The one who controls the past controls the future, said George Orwell;[49] in his masterpiece 1984, Orwell meant that controlling past was about controlling an interpretation of what happened. This has not changed significantly, only the media and technology have changed. The one who owns the capability to control the flow and shape of discourses among social networks or has the capability to mine big data for subsequent huge semantic analysis – and that is not a science fiction today – controls the future. Such military approach has been already widely analyzed[50] and has raised its importance with new technologies. The capability to critically assess this overall knowledge is a defensive capability. When a state and its citizens are resistant to outer manipulation and targeted influence, it should be called a defensive power of a state, its government, its formal constitution and the whole regime – preferably open and liberal democratic regime. Sometimes this defensive power is called "a mental resilience."[51]

[47] (Waltz 1998; Scaparrotti 2012)

[48] (Foucault 1981)

[49] (Orwell 1949)

[50] (Waltz 1998)

[51] Mentioned in a presentation of Jarno Limnéll from McAfee during his presentation on CyCon 2014 organized by CCD COE Tallinn Estonia.

Second, critical knowledge is a critical capability to conduct a successful cyber attack. To be aware of vulnerabilities or available exploits is what matters here; not the overall hacking ability that can be learned, but the combination of hacking ability with the critical knowledge of a specific vulnerability is a strategic advantage. If a hacker needs to learn what vulnerabilities are in a targeted system, he/she is more likely to be uncovered by the operators defending the targeted system. If he/she knows exactly the way how to proceed in; the likeliness of being uncovered decreases significantly. Critical knowledge has several specifics that differentiate it from military capability. First, critical knowledge, as a capacity, is immeasurable. Possessing it does not necessarily mean using it within a military operation; hence, it cannot be assessed as an imminent threat, but rather an opportunity. However, as mentioned above, the fact that such an opportunity is so widely accessible, is a threat itself. Second, having 0-day exploits in systems (already generally unknown vulnerabilities) is unavoidable; thus there will always be a possibility that someone obtains such critical knowledge. The threat is unavoidable. Third, if such vulnerability emerges from general design of the system, to have it means zero investment to obtain it.

3. Offense-defense theory in cyber perspective

ODT is not a consistent theory, but rather a bunch of theoretical approaches that use the term offense-defense principle in its analysis. There are moments in literature when such direct realism works and are proved on empirical basis, and there are moments in interstate conflict that cannot be fully analyzed from such theoretical perspective. That said, it loses sense trying to fully undermine or fully confirm usability of the theory, even though some criticism is astonishingly complex.[52] However, ODT is useful in the crucial point of this paper; in the assertion that accumulation of offensive power may lead to war. I argue that accumulation of critical knowledge in cyberspace combined with the attribution problem will silently escalate to a wider conflict that should be called war; as already argued above. Additionally, the conflict between Ukraine and Russia that sparked in 2014 showed that even in a conventional war the attribution problem plays significantly into the hands of the attacker who constantly refuses involvement in the conflict. Hence, the contemporary problem in recognizing a war in international relations is merely linked to the attribution problem, no regards whether it is in cyberspace or within physical territory.

There are two distinct, but somehow communicating lines in ODT theory. The first contends that war or international conflict is much more likely to outbreak when offense dominates defense, when offense has the advantage over defense; conversely peace is more probable when defense dominates offense.[53] The second one contends that differentiation of military postures and weapons is useful and possible.[54]

[52] (Shiping 2010)

[53] (Quester 2002; R Jervis 1978)

[54] (Glaser and Kaufmann 1998; Lynn-Jones 1995)

The prevalent part of the ODT debate is strictly oriented on military analysis and thus analysis of military advantage. The introduction of the theory by Robert Jervis that different military capabilities and their orientation to offense or defense may trigger security dilemma between states laid down the basis of this classic realistic debate.[55] Further arguments that the division between offensive and defensive systems cannot be simply distinguished led to the answer by Glaser and Kaufman who offered a perspective of offense-defense balance (ODB) measurable as a cost-ratio of offense to defense.[56] There are factors influencing ODB. Those factors are either narrow or broad. The former consists only of technology and geography; the latter was developed by Glaser and Kaufman and includes additionally the size of force and cumulative resources.

However, critics have raised their arguments on immeasurability of those factors; impossibility of their combination or that the combination itself lowers possibility to use ODT. The most detailed criticism to the author's knowledge has been developed by Shiping Tang who argues that while the factors are correctly in place in argumentation about their influence to ODT, they do not enable measurability of ODB.[57] In that perspective, ODT cannot contribute to evaluation whether a state tends to offense another state. However, the point of this article is that in cyberspace, offense dominates defense with no regards whether the initiator is a state or non-state actor. This brief application of ODT is thus the third important conclusion of this article that escalation of conflict, where there is a strategic objective, is inevitable. Explanation follows.

Jervis belongs to scholars who argue that nuclear deterrence has shifted the offense-defense balance toward defense. A state that performs an operation with the aim to conquest a nuclear state would usually destroy itself;[58] thus the cost ratio achieved its maximum. This applies until the offensive state decides to conduct an operation in which the reliability of source identification from which the operation was initiated is close to impossible. This is well known and already explained attribution problem in cyberspace.[59]

Just the fact that both types of cyber operations drawn above (IOps or cyber attacks against ICTs using critical knowledge) are not reliably attributable to its origin favors offense. In that perspective, it does not matter whether ODT helps us to measure offense-defense balance, because the power in cyberspace is for sure immeasurable, but it shows us under what circumstances the escalation occurs. There is no way how to deploy satellites for mapping deployed military assets. The advantage is not in the physically detectable firepower, but in *instant critical knowledge* of particular vulnerabilities; instant because vulnerabilities are patched on an ordinarily basis. If we define cyberspace or territory as a bunch of IT systems directly connected to control some key systems such as those that run critical infrastructure, then space is defined as a network of interconnected nods rather an area or land. Taking control

[55] (R Jervis 1978)

[56] (Glaser and Kaufmann 1998)

[57] (Shiping 2010, 235)

[58] (R Jervis 1978)

[59] (Mudrinich 2012)

over those systems means taking control over that territory; it means conquest. The means of such control is the critical knowledge, the second one we mentioned above, the knowledge that is not a general knowledge of such systems, but the knowledge that includes its highly specific configuration and settings. Knowing configuration and settings that led to taking control over a power grid including power plants within a specific territory is certainly a conquest of that facilities on a particular territory.

The fourth important point of this paper that gets back to the debate over a war focuses at the moment when having a control of critical infrastructure, even though a remote one, is with no doubt an intervention and that the long-lasting campaign is a cyber war.

3.1. Super-empowering by the critical knowledge

Having power to take control over a sovereign territory of a state (land) by military force means having assets such as tanks and capability to build them. Such capability usually belongs to states – individuals do not have knowledge and capacity to design and produce such specific equipment. In contrast to our previous explanation, an individual can have knowledge and capability to control a territory using cyberspace represented by some network of systems that compose critical infrastructure. Such a critical knowledge super-empowers directly individuals, thus non-state actors; it may empower states, but indirectly. The fact that states will exploit the attribution problem in the future, as no isolated cyber attack has been attributed to any state to date (Syria 2007 was attributed to Israel, just because the link between the cyber attack and the air strike by jets was apparent), puts any future operation of a state to the dimension of a non-state actor. Therefore the international law would not be useful to stop or deter any state in doing so.

First, if any offense-defense balance factor were ever measurable, e.g. the firepower of conventional military assets, they would definitely not be measurable with interface using cyberspace. Hacking into UAVs has already been recorded in recent history[60] and such critical knowledge – where UAV has critical vulnerability to be exploited – completely destroys any argument of ODB.

Second, such critical knowledge can be sold to whoever has general capacity in IT systems. I argue that hacking UAVs is not about decades-long practice in hacking, but rather about mind brightness to exploit a completely unknown vulnerability that is a used feature in other situations[61] and about a critical knowledge that particular vulnerability is available to do it. Having completely bullet-proof IT systems is thus unachievable.

Third, it is not a state, but individuals who posses such critical knowledge which super-empowers them even in a situation when the individual works for a state. Such knowledge may

[60] (Telegraph 2011)

[61] USB can be hacked even though it is completely empty. Hacking firmware of USB stick can switch it from memory storage to keyboard for computer to which it is connected. Such switch is undetectable for any antivirus or other antimalware programs, but computer uses directly a hacked firmware which can have other implemented and hidden features.

not be transferable to any person easily if the individual developed an exploit into a tool that has to be used somehow.

Fourth, if you have the critical knowledge, you do not need to develop, invent or disclose it to execute it; your cost of using your power is close to zero; however developing or obtaining a critical knowledge would be cheaper than developing and producing a conventional military firepower. If we take the example of UAVs, hacking them and keeping such hacking capability (keeping the needed critical knowledge updated) is significantly cheaper than having a complex anti-air missile system to take them down from the sky. The same critical knowledge may be in the hands of a non-state actor. Hence we would face in the near future more attacks with less traditional violence that are less costly, but comparably serious.

Fifth, if there is no reliable way to be sure about the origin of a cyber attack exploiting a critical knowledge, we can be sure that such environment will escalate. This conviction lies in the offense-defense theory, in part, which I believe works. States (as entities) with less defensible borders tend more to expansionism. In that perspective, cyberspace does not have distance, nor it has appropriate borders of "territorial areas"; all destinations are available with no regard to physical distance, which creates an environment where conventional temporality is replaced with near instantaneity.[62] Territories are rather networks than defensible areas and those networks are hard to defend. Selected networks are likely to be much more defended that the whole cyberspace.[63] However, the argument of critical knowledge makes any system an easy target with no regards on its defence.

3.2. Active cyber defence as an evidence of offense domination

The debate on defensive methods of IT systems has come to the point of general consensus that those systems are by design indefensible. Policy reaction of the European Union would serve to this finding as the whole strategy in cyberspace, for the EU focuses strictly on systems resilience rather then system defence.[64] In such environment where defence is worthless, a new concept of *"active cyber defence"* has been developed. The active cyber defence consists of activities such as detection, deception and termination.[65] Detection e.g. detects anomalies in the network and would serve as a support measure for further decisions and actions. Deception systems are about catching a hacker in a honeypot environment while the hacker thinks he/she is in the real system. It serves for learning about hacker's capabilities and knowledge as the operator can observe what the hacker is doing. Termination is counter-hacking the hacker's systems.

The whole active cyber defence usually focuses on learning what the attacker is doing during the operation against us; then it proceeds to a counter-attack against the hacker. The whole "kill-chain" during each active defence operation leads into an operation, which in its

[62] (Choucri 2012, 4)

[63] (Libicki 2007, 276)

[64] (EU 2013)

[65] (Lachow 2013)

principle is an offensive action. Hence calling such activity defensive is ultimately an euphemism and conversely confirms that offense dominates defence in cyberspace.

4. Conclusion

This paper offers reasoning why the concept of war should be reconceptualized according to new realities in cyber security. The debate over such conceptualization is currently very hot, hence, this article briefly wanted to contribute into this debate by contention that violence in cyberspace may be on the one hand only indirect, but on the other it is definitely qualified. It means that used force is transforming into a specific power. This institutionalization of power is weak at the moment, but we can observe an intense development. However, the first part concluded with the assertion that lethality is not a necessary precondition for calling a conflict a war; violence can have different shapes, non-lethal, coercive, but still with military strategic intentions. If an operation in cyberspace is a prerequisite for a wider campaign and thus can be understood as a part of such campaign; if it lasts for a long time and violates sovereignty of particular states intervening into their territory, then it is supposed to be called a war. Another concept, sovereignty, is not accepted well in cyberspace, but this moment waits for the state practice to develop customary law in international law. Another mentioned concept(s), space-territory-cyberspace was conceptualized with a meaning of conquest; where conquest means having control over people and assets in the argeted territory. Territory in cyberspace was thus conceptualized through an attack that may lead to taking control over critical infrastructure of a particular state or influencing and changing minds of people within that territory by IOps.

Additionally, means of power in a critical knowledge and capability to influence general knowledge of the outer reality – a world, have been explained as two new kinds of power recognizable in cyberspace as significant. Power in critical knowledge serves in super-empowering non-state actors at first; however, an argumentation has been examined why states should be approached as non-state actors as well. They will very likely tend to exploit the attribution problem in cyberspace, hence any international law will not serve as a mitigation means of possible international conflict.

All above-mentioned concepts along with this new kind of power have been used in the analysis of offense-defence debate and applied to cyberspace to show that offense will certainly dominate defence. Several arguments have been proposed to support this thesis with policy euphemism called active cyber defence which is a pure offensive policy at a glance.

However, four important points or arguments why the conflict in cyberspace will tend to escalate have been made.

First, we examined a debate about a concept of war from the perspective of classical thoughts of Clausewitz and criticized the approach of Thomas Rid. The most important findings were that violence does not need to be lethal to be part of a military strategy of warfare; that a latent violence prevails in cyberspace and that such violence is indirect and qualified; thus such violence is supposed to be understood as a precondition for war from the Clausewitzian perspective. We found instrumentality in cyber war and we argued that the combination of instrumentality with latent violence would constitute an operation with political nature. All those arguments were developed as a criticism of the popular Rid's assertion that cyber war will not take place. Second, states do and will tend to exploit the attribution problem to their strategic advantage; hence they will have so-called dual interest in shaping a future regime of cyberspace. The actors will not be labelled, so states will not be responsible and the attacked state has to treat such an aggressor as a non-state actor. Third, the assertion that offense dominates defence in cyberspace would lead to a possible escalation. Fourth, having a control over critical infrastructure or just trying to take over such control is supposed to be recognized as an intervention and violation of state sovereignty and should trigger appropriate clauses in international law; especially right to defence, as even though as an appropriate one according to international law – a clause of proportionality. However, all these three points, I believe, are strong arguments as to why the conflict in cyberspace will escalate.

References

Arendt, Hannah. 1972. "On Violence." In *Crises of the Republic*, 105–98. San Diego, New York, London: Harcourt Brace Jovanovich.

Bartelson, J. 1995. *A Genealogy of Sovereignty*. Cambridge Studies in International Relations. Cambridge University Press. http://books.google.cz/books?id=w-5wQgAACAAJ.

Bauman, Zygmunt. 2000. *Liquid Modernity*. *Contemporary Sociology*. Vol. 30. doi:10.2307/3089803.

Blank, Stephen. 2008. "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy* 27 (3): 227–47. doi:10.1080/01495930802185312.

Brodie, B. 1946. *The Absolute Weapon: Atomic Power and World Order*. Harcourt, Brace and Company.

———. 1959. *Strategy in the Missile Age*. G - Reference, Information and Interdisciplinary Subjects Series. RAND Corporation.

Buzan, B, O Wæver, and J de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers. http://www.google.cz/books?id=j4BGr-Elsp8C.

Cavelty, Myriam Dunn. 2008. "Cyber-Terror—looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology & Politics* 4: 19–36. doi:10.1300/J516v04n01_03.

———. 2012. “The Militarisation of Cyberspace: Why Less May Be Better.” In *4th International Conference on Cyber Conflict*, edited by Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, 141–53. Tallin: NATO CCD COE.

CCDCOE. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Edited by Michael N. Schmitt. New York: Cambridge University Press.

Choucri, N. 2012. *Cyberpolitics in International Relations*. Cambridge, Massachusetts and London, England: MIT Press. http://books.google.cz/books?id=N7iNQSj-X84C.

Clausewitz, C, M Howard, P Paret, and B Heuser. 2007. *On War*. Oxford University Press. http://books.google.fr/books?id=K5FKjjsbXBcC.

Collins, Sean, and Stephen McCombie. 2012. “Stuxnet: The Emergence of a New Cyber Weapon and Its Implications.” *Journal of Policing, Intelligence and Counter Terrorism* 7 (April): 80–91. doi:10.1080/18335330.2012.653198.

Cox, Noel. 2002. “The Regulation of Cyberspace and the Loss of National Sovereignty.” *Information & Communications Technology Law* 11 (3): 241–53. doi:10.1080/1360083022000031920.

D’Entreves, Alexander Passerin. 1967. *The Notion of the State*. London: Oxford University Press.

Deibert, Ronald. 2009. “The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace.” In *The Routledge Handbook of Internet Politics*, edited by Andrew Chadwick and Philip N. Howard, 1st ed., 512. Taylor & Francis. http://books.google.com/books?hl=en&lr=&id=GJdfuGSa1xUC&oi=fnd&pg=PA323&dq=The+geopolitics+of+internet+control+Censorship,+sovereignty,+and+cyberspace&ots=dVmgsv6NwT&sig=e40cAmLWgcClGCY0J_HjE0sQefQ.

EU. 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels. http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

Foucault, Michel. 1981. “The Order of Discourse.” In *Untying the Text: A Post-Structuralist Reader*, edited by Robert Young, 48–78. London and New York: Routledge.

Franzese, PW. 2009. “Sovereignty in Cyberspace: Can It Exist.” *AFL Rev.* 64: 1–42. http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid,url&db=a9h&AN=45162330&lang=cs&site=ehost-live.

Gartzke, Erik. 2013. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38 (2): 41–73. http://belfercenter.ksg.harvard.edu/files/IS3802_pp041-073.pdf.

Glaser, Charles L, and Chaim Kaufmann. 1998. “What Is the Offense-Defense Balance and Can We Measure It?” *International Security* 22: 44–82. doi:10.1162/isec.22.4.44.

Herrera, Geoffrey L. 2006. “Cyberspace and Sovereignty.” *Conference Papers -- International Studies Association*, 1–34. http://search.ebscohost.com/login.aspx?direct=true&db=poh&AN=27205425&site=ehost-live.

Jervis, R. 1978. “Cooperation under the Security Dilemma.” *World Politics*. http://journals.cambridge.org/abstract_S0043887100016191.

———. 1989. *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Cornell Paperbacks. Cornell University Press.

Jervis, Robert. 1988. “The Political Effects of Nuclear Weapons A Comment.” *International Security* 13 (2): 80–90.

Kahn, H. 1960. *On Thermonuclear War*. University Press.

Kaiser, Robert. 2015. “The Birth of Cyberwar.” *Political Geography* 46: 11–20.

Krause, Keith. 2009. “War, Violence and the State.” *Securing Peace in a Globalized World. London: Palgrave Macmillan*.

Lachow, Irving. 2013. “Active Cyber Defense - A Framework for Policymakers.” http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.

Lewis, James A. 2010. “Sovereignty and the Role of Government in Cyberspace.” *Brown Journal of World Affairs* 16: 55–65. http://search.ebscohost.com/login.aspx?direct=true&db=poh&AN=50883224&site=ehost-live.

Libicki, Martin. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press. http://books.google.cz/books?id=QUYMwJR5pYMC.

Lieber, Keir A, Daryl G Press, David Kang, Christopher Layne, George Lewis, Jennifer Lind, and Daniel Lindley. 2006. “The End of MAD ?” *International Security* 30 (4): 7–44.

Lynn-Jones, Sean M. 1995. “Offense-Defense Theory and Its Critics” 1 (4): 59–63.

McDermott, Roger. 2014. “Russia’s Information-Centric Warfare Strategy: Re-Defining the Battlespace.” *Eurasia Daily Monitor, The Jamestown Foundation* 11 (123). http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=42594&no_cache=1#.VGtzz1PF_bk.

Mudrinich, Erik M. 2012. “CYBER 3.0: THE DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE AND THE ATTRIBUTION PROBLEM.” *Air Force Law Review* 68: 167–206. http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid,url&db=a9h&AN=77789094&lang=cs&site=ehost-live.

Orwell, George. 1949. *1984: A Novel*. New American Library.

“Oxford Dictionary Term: ‘Conquest.’” 2015. http://www.oxforddictionaries.com/definition/english/conquest.

Pomerantsev, Peter, and Michael Weiss. 2014. *The Menace of Unreality : How the Kremlin Weaponizes Information , Culture and Money*. New York.

Quester, George. 2002. *Offense and Defense in the International System*. Transaction Publishers. http://www.google.cz/books?id=GVyuYeBGKHcC&pgis=1.

Rid, Thomas. 2012. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35 (1). HURST C & Company PUBLISHERS Limited: 5–32.

———. 2013a. *Cyber War Will Not Take Place*. Hurst. http://books.google.cz/books/about/Cyber_War_Will_Not_Take_Place.html?id=ZvDQlAEACAAJ&pgis=1.

———. 2013b. “More Attacks, Less Violence.” *Journal of Strategic Studies* 36 (1): 139–42. doi:10.1080/01402390.2012.742012.

Sakharov, A D, and H E Salisbury. 1968. *Progress, Coexistence and Intellectual Freedom*. Pelican Series. Penguin Books. http://books.google.cz/books?id=15EkAQAAMAAJ.

Sauer, Tom. 2009. “A Second Nuclear Revolution: From Nuclear Primacy to Post-Existential Deterrence.” *Journal of Strategic Studies* 32 (5): 745–67. doi:10.1080/01402390903189402.

Scaparrotti, Curtis M. 2012. “Joint Publication 3-13 Information Operations.” Joint publication. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

Schelling, Thomas C. 1966. “Arms and Influence.” *American Sociological Review*.

Schmidt, Nikola. 2014. “Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War.” *Defense and Strategy*. doi:10.3849/1802-7199.14.2014.02.073-086.

———. 2015. “A Sociological Approach to Cyberspace Conceptualization and Implications for International Security.” In *Perspectives on Cybersecurity*, edited by Jakub Drmola, 77–77. Brno: Muni Press.

Schneider, Mark. 2008. “The Future of the U.S. Nuclear Deterrent.” *Comparative Strategy* 27 (4): 345–60. doi:10.1080/01495930802358539.

Shiping, T. 2010. “Offence-Defence Theory: Towards a Definitive Understanding.” *The Chinese Journal of International Politics* 3 (2): 213–60. doi:10.1093/cjip/poq004.

Stone, John. 2013. “Cyber War Will Take Place!” *Journal of Strategic Studies* 36 (1): 101–8. doi:10.1080/01402390.2012.730485.

Telegraph, The. 2011. “Iran Says Captured US Drone Is Their ‘Property’ Now.” http://www.telegraph.co.uk/news/worldnews/middleeast/iran/8952827/Iran-says-captured-US-drone-is-their-property-now.html.

US-DoD. 2011. *DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE*. http://www.defense.gov/news/d20110714cyber.pdf.

Waltz, Edward. 1998. *Information Warfare Principles and Operations*. *Information & Security: An International Journal*. Vol. 2. Boston, London: Artech House. doi:10.11610/isij.0212.

Wright, Quincy. 1983. *A Study of War*. Vol. 15. Chicago: University of Chicago Press.