future internet

MDPI

Article

Cyber Conflicts as a New Global Threat

Alexander Kosenkov

Information Society Research Center, Chernihiv 14000, Ukraine; cybersecresearch.ua@hotmail.com; Tel.: +380-930570382

Academic Editor: Jiankun Hu
Received: 7 June 2016; Accepted: 5 September 2016; Published: 9 September 2016

Abstract: In this paper, an attempt is made to analyze the potential threats and consequences of cyber conflicts and, in particular, the risks of a global cyber conflict. The material is based on a comprehensive analysis of the nature of cyber conflict and its elements from both technical and societal points of view. The approach used in the paper considers the societal component as an essential part of cyber conflicts, allowing basics of cyber conflicts often disregarded by researchers and the public to be highlighted. Finally, the conclusion offers an opportunity to consider cyber conflict as the most advanced form of modern warfare, which imposes the most serious threat and whose effect could be comparable to weapons of mass destruction.

Keywords: cyber conflict; information warfare; cyber warfare; information operations

1. Introduction

During the last decade, global social and political landscapes were changed by the revolutionary development of information and communications technologies (ICT). New ICT has also significantly influenced warfare, among other ways through the emergence of network-centric warfare doctrine and unconventional, hybrid, information, and asymmetric warfare. The most significant transformation brought by the ICT was the emergence of a totally new form of conflict—cyber conflict (in this paper, cyber conflict is defined as conflict with the application of cyberspace capabilities in order to achieve objectives in or through cyberspace)—the rise of which we are witnessing worldwide today. Despite this clear and evident threat, there are still ongoing debates about the existence of cyber warfare. It is obvious that cyber conflicts are the game changers in modern warfare. They brought unprecedented changes incomparable to any preceding them. For instance, cyberspace is the first fully artificial space (no matter within or outside of the information environment) which, alongside land, sea, air, and space is considered to be a domain pursued for military superiority [1].

However, the understanding of cyber conflicts and changes happening in the warfare remains rather superficial. Current research cannot offer a holistic approach to cyber conflict. Its nature is still largely unknown to us [2–7]. As a result, we cannot address the main question of pressing issue today: how dangerous cyber conflicts are and what consequences and threats they bring. The answer to this question will determine not only the further development of military strategies and the international legal regulation of warfare, but also further civil development (both technological and social).

The most dominant current approaches to cyber conflicts are insufficient. As such, this paper concentrates on an effort to provide an alternative and more societal perspective on what cyber conflict is and how dangerous it could be. For this reason, the paper does not pretend to give an exhaustive characterization of cyber conflicts in general, but instead will primarily focus on issues relevant to the under-researched societal aspects of cyber conflicts.

This paper will make an attempt to answer the question of how serious the threat of cyber conflict—particularly global cyber conflict—is, and if we could call it the next challenge for the whole of modern civilization, alongside nuclear warfare. To do this, we first need to understand why the

current approach to cyber conflicts has not yet produced significant results. Secondly, it is important to understand the basic elements of cyber conflicts (CCs) (such as the means of cyber conflicts, MCCs), and also to understand how they are changing warfare. Subsequently, we should understand how warfare has changed in general.

2. Results

2.1. Cyber Conflicts Research Problem

Apparently, and somewhat predictably, the primary problem with existing CCs research is the approach to the research object. While CCs and MCCs have become cutting edge and different from any conflict and weapon in the physical realm, researchers are trying to apply a narrow technical understanding of warfare that worked before CCs and are fastening an old fashioned paradigm when trying to understand the radically different means, methods, objectives, and impacts of cyber conflicts. The old-fashioned coercion-centric paradigm currently dominating in research is deeply insufficient to understand cyber conflicts, as tools have shifted from coercion in its classical form to more advanced means. It is hard to say that the current approach is even partially successful while: (1) there are no reliable mechanisms for cyber conflicts assessment (not on a case-by-case and fact-specific basis [8]); (2) it is still impossible to appropriately evaluate the effects of conflict that do not cause mass casualties and/or destruction [9]; (3) it is unclear how cyber conflicts are interrelated with conflicts conducted with conventional means; (4) it is ambiguous what the potential strategic implications of cyber conflicts could be [9]; (5) legal regulation is based on persistent efforts to interpret existing norms [10], rather than accept the need for special regulation of cyber conflicts like the one for other cyberspace-related issues such as e-commerce and cyber crime. Even information operations could address the use of old "tools", but not CCs. Therefore, the need to identify the basic features that make CCs unique in comparison to physical conflict and impede its research is of primary importance. These features include:

- Fast emergence. CCs have emerged very quickly and are rapidly changing together with ICT, seriously diminishing the application of the historical approach, which is the basic one for military studies. Historical methodology is still important, but only for the period relating to cyberspace. In addition, there are neither sufficient historical materials nor appropriate methodologies to understand the conflict's history, which spans less than 30 years. It is also important that, for this period, no single wide-scale CC has taken place, but only "local" ones (limited to few nations and/or a certain region).
- Insufficient social basis. During the relatively short period of CCs' existence, appropriate institutions and sufficient public knowledge to evaluate the potential of CCs and cope with its threats were not formed. Such a situation could lead to paradoxes, such as the idea that "malicious code has not, so far, generated sufficient harm or damage to warrant serious human rights attention" [11], only because the human right for secure cyberspace had not yet been declared.
- Dependence on the social sphere. CCs' effects depend on the way and degree of integration of ICT into society.
- Complete mediation by cyberspace. This means that an operation is maintained in a totally new landscape existing without familiar time and space dimensions, instead having new "human" dimensions.
- CCs could almost be considered an "ideal conflict", having blurred lines between peace and war, military and civilians, war and crime, and even war and the right for protest. This is leading to the massive weaponization of previously peaceful spheres of life.
- High potential for the broad involvement of non-state actors. Currently, sources needed for participation in CCs or the creation of MCCs are not monopolized by the state or any other social institution, and are not extremely expensive, which could affect their availability to a wide range of persons. Some transnational companies already compete with states for control over

information and ICT services. Occurring simultaneously, the absence of both physical and serious technical barriers gives anyone the ability to use MCCs. Private persons are becoming not only combatants in cyber conflict, but targets as well. Previously, private entities were not primary targets in the conflicts, as they were "unreachable" behind the defense lines created by the state. Now, however, when private organizations are global and each one is reachable through the Internet, private entities are becoming one of the primary targets. As the role of the state in the protection of private person's interests have significantly decreased, it is widely debated who should ensure the security of private information assets in cyberspace: private entities themselves, or the government. The state cannot ensure cyber security for all private persons, while still there is no reliable mechanism to ensure public interests exclusively through private actors. It makes the situation very uncertain. Who will be capable of coping and how will they cope with a serious cyber conflict or crisis in the future?

- Need for the provision of special resources. Unlike previous conflicts, in CCs, there is the need for intellectual, human, and computational resources which are hardly measurable and not yet well managed by the military.
- Complicated nature. Cyberspace as a battle domain does not only interact with physical battle spaces (such as physical battlefields interacting between each other). Cyberspace is deeply integrated with physical battlefields. Exactly for this reason, cyber commands function within Army, Fleet, Air Force, and Marine Forces in the USA [12]. CCs are also tightly linked to cyber-security in general, which means that there is the need for deep private–military cooperation in the sphere of once exclusively military competence. The complicated nature of CCs can be illustrated by the fact that often researchers are hampered in the differentiation of contiguous to CC kinds of warfare (information, hybrid, electronic warfare, etc.).
- Covert nature. CCs are unobservable to the general public, as MCCs could be operated exclusively remotely, and there may be no tangible evidence to prove the involvement of certain adversaries. The general public can only directly observe the effects of CCs, not the conflict itself, which gives wide potential for information manipulation.

On the strength of the features of CCs and the fact that ICT and society are actively converging, we can conclude that CCs have two main elements that we need to consider: technological and social. The technological elements include the classical warfare paradigm dealing with the use of new technical tools and a new medium (cyberspace) to reach traditional military targets with the objective to destroy, disrupt, and/or incapacitate the enemy. As this field is comparatively known to the military doctrine, its main parameters are characteristics of technical means and technologies. The societal element appears in the sphere of military competence as the result of the "blurring of lines" in the cyberspace. It deals not with the infliction of damage or incapacitation, but with the "transformative" use of social means available in cyberspace. In order to go beyond the general characteristics given above, and in order to try to provide more complex evaluations, we need to consider technical and social elements of MCCs separately.

2.2. Technical Elements of Cyber Conflicts

As the technical element of CCs is the first known one, it has the best consideration. It constitutes the application of the technical means of cyber conflicts (technical MCCs), including malicious software and hardware, malicious activities (DDOS (Distributed Denial of Service), hacking, phishing, etc.) and devices controlled with cyberspace means (including those programmed for autonomous operation) to gain superiority in the conflict.

The following features make technical MCCs a weapon of the next generation of warfare:

- Dynamic and changeable nature [13]. Technical MCCs are being developed and changed very quickly. Unlike any kind of weapon, they have not any common form and are limited by minimal constraints.

- Single or limited use [13]. If a technical MCC was used to attack the target, it is highly likely that its characteristics and mechanisms of attack would become known and would be used to build countermeasures, remove vulnerabilities, etc. Only the technical MCCs that are the most innovative and unknown to the adversary will be the most efficient. The longer a technical MCC is used, the lower efficiency it has, and the fewer targets it can hit. It is impossible to develop a universal virus worth billions of US dollars that could be efficiently "deployed" for a few decades to hit different targets. Even the successful use of advanced persistent threat (APT) against a single target for a long time does not guarantee that APT would not be removed tomorrow and that it could be used to hit other targets of high priority.
- High scalability. Technical MCCs could be applied to a target of any scale, from individual pacemakers to critical infrastructures of global significance.
- Unpredictability. Technical MCCs have far more attack vectors and malicious mechanisms to harm the target than conventional weapons. For example, a technical MCC or vulnerability could be deployed in an enemy system covertly and activated at H-hour.
- Unobvious nature of technical MCCs' effect. Technical MCCs by nature do not inflict any direct damage to an object of an attack (e.g., destroy equipment, disrupt communication, etc.). They have their own interim target of influence: artificial data systems, the impact on which will cause damage to the target (whatever it is), information stored in the system or physical objects managed by the system.
- Exceptional nature of technical MCCs. At first glance, especially for the general public [14], the threats of technical MCCs are insignificant in comparison to previous generations of weapons, such as nuclear or space weapons. This makes technical MCCs almost an ideal instrument to use and an issue of serious concern.
- Further complications. Both technical MCCs and protection against them are actively evolving to become more resilient, mutable, adaptive, and smart. These trends also make technical MCCs more autonomous and potentially less controllable. Naturally, they could have only a limited scope of targets, like Stuxnet had. However, that does not exclude the potential application of broad-spectrum uncontrollable destructive technical MCCs, as such attacks have also shown their efficiency.
- Clandestine operation. Due to cyber battlespace peculiarities, the majority of technical MCCs are built to operate covertly. This means that not only the operation itself, but also its consequences could be unnoticed for a long time. That makes the "fog of cyber conflict" even more dense.
- Recoverability of damage and time-limited effect. Technical MCCs could disrupt, incapacitate, or destroy critical infrastructure, but in the most cases "homefield advantage" gives a defending party an opportunity to repair the damage and rebuild technical protection in the short term.
- Offensive nature [15]. In the case of nuclear weapons, their immense destructive power makes them offensive. As for technical MCCs, we can say that their offensive nature is rooted in unpredictability and their broad, unmanageable effect.

Any of these features separately does not seem to be a radical game-changer for warfare, but when combined into a single means of warfare, they can lead to the transformation of the nature of modern conflict. In particular, these characteristics combined make the basic pillars and mechanisms of modern peace inapplicable in the case of CCs. Arms control and non-proliferation were basic for the reduction of escalation during the Cold War, but how can the means of cyber conflicts be controlled if they have no physical guise, if you cannot detect their deployment in most cases, if they do not demand significant resources to be built, and when intelligence gathering about them is hampered, even today? However, there are no alternative mechanisms that could be used to settle the application of technical MCCs. Uncertainty regarding technical MCCs rises even more if we take into account that the buildup of cyber capabilities is non-linear and quite unpredictable, due to the peculiarities of the

required resources. These problems significantly reinforce mutual distrust among potential parties of the CCs.

As more progressive mechanisms of peace preservation are inoperative, we should try to get back to the doctrine of mutually-assured destruction and rational deterrence theory, which also appear to be obsolete. Adversaries could only assume that the defending party could retaliate against large-scale cyber attacks both with technical MCCs and military options to annihilate the attacker, but still they cannot be entirely sure. There may be no rational deterrent threat while reliable evaluation mechanisms for technical MCCs are absent. As Martin Libicki wrote: "The current paucity of attacks has nothing to do with the fear of retaliation and more to do with the inability of other states to generate a sufficiently interesting capability or a sufficiently pressing opportunity" [9]. So, what will make non-measurable capabilities "interesting" and "opportunity pressing"? The creation of a "cyber triad capability" equivalent to a nuclear triad [16] cannot help to achieve credibility of cyber deterrence for the same reason—absence of reliable evaluation of an enemy's capabilities. Deterrence theory also looks to be inapplicable for a few other reasons. Firstly, due to the inability to identify an attacker clearly, borderless cyberspace could allow the launch of distributed attacks from any part of the world, including the territory of the defending state; Secondly, it is unclear how this retaliation mechanism would work in the case of an attack being launched by a non-state actor; Thirdly, it is currently unclear when a retaliation mechanism should be launched, where the red line is defined, and even which attacks are considered to be large-scale.

All aforementioned factors certainly trigger further exponential build up of cyber capabilities and a "cyber arms race" that could be far more threatening and massive in comparison to a conventional "arms race". We could consider only a few factors that confirm that assumption. The number and variety of means potentially applicable in a "cyber arms race" is unprecedented. The process of weaponization is truly massive, starting from putting backdoors to any equipment, software, and any electronic device, and ending with the weaponization of the Internet. We can only imagine what effects this arsenal could have in case of its full-scale application. Low demand for the material resources necessary to build technical MCCs will mean that the number of constraints for the development of technical MCCs will also be maximally low. This does not mean that all of the actors will be able to develop highly efficient technical MCCs, but all of them could definitely try to create their own cyber arsenal. The creation of nuclear arsenals has been accompanied by public attention, non-proliferation education campaigns, and civic controls that hinder the arms race with social mechanisms. In the absence of an explicit and directly perceptible threat from cyber arsenals, it is doubtful that the growth of cyber arsenals will cause such social resonance in the future.

Finally, the high velocities of CCs and the large number of operated technical MCCs will demand the application of automated intelligent control systems that will be able not only to retaliate (like the Soviet/Russian "Dead Hand" system that is capable of automatically triggering the launch of intercontinental ballistic missiles under certain conditions), but possibly also to strike first under different scenarios. This significantly increases the unpredictability and threats of CCs.

To all of the above, the doctrine of military response to large-scale cyber attacks reanimates the threat of global conventional war triggered by unpredictable cyber conflict.

Technical MCCs potentially have a unique application strategy: the infliction of organizational damage in order to cause state failure, humanitarian crisis, or any other state of enemies' incapacitation. Unlike conventional military attack, the application of technical MCCs could become ideal to avoid large scale military conflict, while successfully neutralizing the enemy nation as a single social organism. However, such a strategy for the application of technical MCCs' could be successful against outsiders in the competition for superiority in cyberspace. At the same time, the infliction of organizational damage with social MCCs (considered in the next section) could be successfully applied against any adversary.

2.3. The Social Element of Cyber Conflict

As mentioned earlier, cyberspace has made the social sphere within it an accessible and therefore obligatory field of military operation. As military operations have shifted from exclusively hard power to a mix of hard and soft power application, soft power operations in the social sphere are an integral part of modern warfare. Simultaneously, it has made social mechanisms more applicable as means for achieving military goals, and it has also made society a more reachable target than ever before. For these reasons, we will determine social means of cyber conflicts (social MCCs) as any means available in or through cyberspace (informational, psychological, technical, etc.), those that use social mechanisms to inflict any societal influence (both in cyberspace and outside of it).

The application of social MCCs is already not an option, but rather a necessity, since the Internet creates a single borderless information space and simultaneously undermines state sovereignty [17]. While losing traditional mechanisms of social control, state actors are trying to regain it with newly available tools and try to compete for the single informational space, while experiencing political crisis due to the gradual erosion of sovereignty.

One of the basic and main directions of the application of social MCCs is anti-government: the disorganization of governance, organization of anti-government protests, delusion of the adversary's population, public opinion influence, and the reduction of an opponent's will to resist [18]. Nowadays, the application of social MCCs goes far beyond this anti-government vector. They are also targeting society in general to make it incapable of restoring and restructuring "damaged" governance.

The war of ideas was one of the key strategic elements that led to the end of the Cold War. Alongside the ideological battle, the main actors during the Cold War also applied subversion of any kind, ranging from informational to the support of armed groups, and often both of these notions converged deeply. The strategy of subversion in proxy wars in third world countries was especially successful: coups and revolutions were happening in different parts of the world. There were even well known, unsuccessful examples of (ideologically motivated) active armed subversion in countries belonging to one of the blocks, such as Red Brigades, Red Army Faction, etc. Large-scale armed subversion has never broken up on the territory of the USSR or the USA due to strong social regulation (maintained by the official state institutions) and social self-regulation. The mechanism of social regulation inter alia is based on the ability of state institutions to fully control informational space and flows and determine social conditions. The social-self regulation is the ability of social institutions to remove, alter, or neutralize unwanted social elements through social pressure and other mechanisms.

Cyberspace has changed both of these mechanisms: information is no longer fully controllable by the state, social space is also gradually becoming global, and people interact through social institutions in cyberspace rather than offline. In the Internet era, fewer and fewer local factors have influence, but more and more social factors originating from the global cyberspace influence social behavior, and consequently, social structure. In a practical military sense, it means that there is great potential to influence the emergence and activity of different social groups on the adversary's territory. During the Cold War, even very scarce influence and resources allowed the initiation of armed subversion and terrorist activities, such as those mentioned before. Cyberspace enables wide informational, social, ideological, and even financial support for subversive groups, and simultaneously disables social regulation and self-regulation that make subversion ultra-efficient both in quantitative and qualitative aspects.

Despite this, the application of social MCCs is not widely considered; however, there is open source information that the main competitors in cyberspace already have corresponding systems at their disposal. Between February–March 2011, mass media published information that the United States Department of The Air Force in June 2010 placed an order for "persona management software" for 50 users, each of which will manage 10 personas. According to published information, each persona should have "background, history, supporting details, and cyber presence that are technically, culturally and geographically consistent. Personas must be able to appear to originate in nearly any part of the world and can interact through conventional online services and social media platforms.

The service includes a user friendly application environment to maximize the user's situational awareness by displaying real-time local information" [19]. In August 2012, a Russian newspaper "Kommersant" published an article alleging that in January 2012 the Foreign Intelligence Service of the Russian Federation announced three "closed" tenders for the development of special software solutions with code designations "Dispute", "Monitor-3", and "Storm-12" [20]. The purpose of the "Dispute" system was described as "research processes of formation of communities of information dissemination internet-centers in social networks" so as to "determine factors of information popularity and distribution". System "Monitor-3" should be created to ensure the "development of methods of organization and management of virtual internet community of involved experts, covering assignment of tasks, control of operation in social media and regular obtainment of information in specified fields from involved experts." Finally, system "Storm-12" would be "a special software package of automated dissemination of information in large social networks and organization of informational support of measures according to prepared scenarios of influence on specified mass audience of social networks".

Information regarding both the American and the Russian solutions is very basic, but nevertheless it is important as a declaration of interest to the application of such systems. Similar but maybe less-advanced systems are already used by large corporations (e.g., social media command centers) and owners of social bot networks for social media monitoring and "promotion" of information. As recent studies show, even the manipulation of the functionality of a web service could inflict serious social effect (like how manipulations of the Facebook information feed caused "massive-scale emotional contagion" [21]). The fact that both solutions were ordered from private companies also confirms the threat of potential wide involvement of non-state actors to both technical and social elements of CCs.

The cases of the application of social MCCs are very rarely considered, because effects of their application are difficult to identify and measure. Nevertheless, there is open source information about such cases. One of them is "social cyber-attack" during the violent events in Assam (India) in July 2012 according to the research by Rebecca Goolsby [22]. Then-unknown persons exploited the high velocities and trusted nature of cyber communications to embed false information in message flows in order to foment strife and undermine stability. The author does not give any details on the mechanism of the attack, but the fact that those events were recognized as "social cyber attack" is very important.

It is apparent that social MCCs are dynamic, hardly traceable, clandestine, and offensive in their nature. Their worst threat is that unlike technical MCCs, their effect could have a strategic significance which is hardly predictable, unlikely scalable, and barely controllable—even in the case of insignificant (at first sight) application. For example, the spread of destructive ideologies or views with the purpose of subverting the enemy could cause global consequences in the long run. However, the social sphere of cyberspace and its interaction with society are still under-researched, and it is difficult to give any assessments regarding the application of social MCCs.

3. Discussions

Both technical and social means of cyber conflicts absorb and advance features of weapons of previous generations, making cyber conflicts—and particularly global cyber conflict—a serious threat to modern society. Key features of cyber conflicts are profoundly different from the features of conventional conflicts (see Table 1), simultaneously making the face of war less brutal, but its essence even more dangerous.

In the worst case scenario, the maximum application of cyber capabilities could supersede effects of all kinds of modern weapon, due to the potential impact on weapon systems and the strategic destructive influence on society. Further analysis of cyber conflicts goes far beyond mathematical models or classical analysis. It demands a more precise, comprehensive, applicable, and transdisciplinary approach. Beyond a brand new approach in the research of cyber conflicts, we also need an innovative and proactive approach in politics and an interaction between cyber conflict research and regulation. Cyberspace and cyber conflict are too dynamic to be regulated with the use of

usual approaches. Apparently, in our modern Information Era, a return to the control of information on a national level would be obsolete. Still, the demand for new regulatory institutions is not met on any level, neither national, nor international. There is no other obvious solution to the problems linked with the threat of cyber conflicts and the means of cyber conflicts, demanding the active development of alternative solutions based on research results.

Table 1. Summary table.

Feature	Conventional Conflict	Cyber Conflict
Primary means	Coercive, destructive	Non-coercive, transformative
Conflict structure	Centralized	Potentially ultra-decentralized
Form	Fixed	Mutable
Delimitation of war and peace	Present	Absent
Dynamics	Medium	High
Timeframe	Precise	Vague
Involvement of private interests	Medium	High
Participation of non-state actors	Medium	High
Capability for differentiation of targets	Medium	Low
Control of conflict means (in the case of massive strike)	High	Low
Intelligence, adversary's capabilities assessment	Efficient	Hampered
Military planning	Efficient	Hampered
Deterrence mechanisms	Present	Absent
Public perception of conflict	Direct	Mediated
Potential for deception regarding the conflict	Low	High
Existence of efficient social and legal mechanisms applicable to the conflict	Present	Absent
Infliction of direct social effect	Absent	Present

We definitely need to better understand what cyber conflict is and what its means are. For this, the development of a terminological apparatus is basic and crucial. The other important direction of further research is potential approaches to the analysis of cyber conflicts and their means, including the classification of the means of cyber conflicts. The classification of the means of cyber conflict into two groups offered in this paper is merely a starting point, but it is definitely one of the variants to better understanding the nature of cyber conflicts. In particular, the classification is important to assume that the most dangerous damage that could be inflicted through cyberspace is organizational and functional, and not a physical one. However, this assumption requires further evidence and more detailed study.

The concept of the social means of cyber conflict due to its newness also needs closer attention and rigorous approach. First of all, in order to prove its consistency, there is a need to understand how exactly the social means of cyber conflicts differ from information warfare maintained through cyberspace and the particular threats of such means of conflict.

The means of cyber conflicts are probably the first means of warfare in human history that humanity possesses and applies but still does not fully understand and control. It makes cyber conflict research not just an auxiliary part of warfare, but its essential component.

Conflicts of Interest: The author declares no conflict of interest.

References

1. U.S. Department of Defence. *Joint Publication 3–12 (R) Cyberspace Operations*; U.S. Department of Defence: Washington, DC, USA, 2013; pp. 1–2. Available online: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (accessed on 1 May 2016).
2. Carr, J. *Inside Cyber Warfare: Mapping the Cyber Underworld*; O'Reilly Media Inc.: Sebastopol, CA, USA, 2011; pp. 1–14.
3. Rosenzweig, P. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*; Praeger: Santa Barbara, CA, USA, 2013; pp. 15–73.
4. Sutherland, B. *Modern Warfare, Intelligence and Deterrence*; John Wiley & Sons Inc.: Hoboken, NJ, USA, 2011; p. 320.
5. Ducheine, P.A.L.; Schmitt, M.N.; Osinga, F.P.B. *Targeting: The Challenges of Modern Warfare*; T.M.C. Press: The Hague, The Netherlands, 2015; p. 293.
6. Zetter, K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*; Crown Publishers: New York, NY, USA, 2014; p. 448.
7. Schmitt, M. Classification of Cyber Conflict. *J. Confl. Secur. Law* **2012**, *17*, 245–260. [CrossRef]
8. U.S. Department of Defense. The Department of Defense Cyber Strategy. 2015; Available online: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed on 1 May 2016).
9. Libicki, M. *Cyberdeterrence and Cyberwar*; RAND Corporation: Santa Monica, CA, USA, 2009.
10. Schmitt, M.N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*; Schmitt, M.N., Ed.; Cambridge University Press: Cambridge, UK, 2013.
11. Casey-Maslen, S. *Weapons under International Human Rights Law*; Cambridge University Press: Cambridge, UK, 2014; pp. 305–307.
12. Stratcom.mil. U.S. Cyber Command—U.S. Strategic Command. 2016. Available online: https://www.stratcom.mil/factsheets/2/Cyber_Command/ (accessed on 1 May 2016).
13. Denning, D. Assessing Cyber War. In *Assessing War: The Challenge of Measuring Success and Failure*; Blanken, L., Ed.; Georgetown University Press: Washington, DC, USA, 2015; pp. 266–284.
14. Korwitts, K. Are Americans Worried about Their Cybersecurity? 2015. SurveyMonkey Blog. Available online: https://www.surveymonkey.com/blog/2015/02/05/americans-worried-cybersecurity/ (accessed on 1 May 2016).
15. Ongstad, M. Cyber-Warfare: Offensive vs. Defensive Balance, 2015. Security Zap. Available online: http://securityzap.com/cyber-warfare-bounded-chaos/ (accessed on 1 May 2016).
16. Sharma, A. Cyber Wars: A Paradigm Shift from Means to Ends. *Strateg. Anal.* **2010**, *34*, 70–71. [CrossRef]
17. Taylor, S. Erosion of National Sovereignty by 21st Century Technology, 2003. International-Business-Center. Available online: http://international-business-center.com/international_business_resources/Sovereignty.pdf (accessed on 1 May 2016).
18. Jaitner, M. Russian Information Warfare: Lessons from Ukraine. In *Cyber War in Perspective: Russian Aggression against Ukraine*; Kenneth, G., Ed.; NATO CCD COE Publications: Tallinn, Estonia, 2015; p. 89.
19. Sherman, E. So, Why Does the Air Force Want Hundreds of Fake Online Identities on Social Media? [Update], 2011. Cbsnews. Available online: http://www.cbsnews.com/news/so-why-does-the-air-force-want-hundreds-of-fake-online-identities-on-social-media-update/ (accessed on 1 May 2016).
20. Barabanov, I.; Safronov, I.; Chernenko, E. Intelligence by The Bot, 2012. Kommersant. Available online: http://www.kommersant.ru/doc/2009256 (accessed on 1 May 2016).
21. Kramer, A.; Guillory, J.; Hancock, J. Experimental evidence of massive-scale emotional contagion through social networks. *Proc. Natl. Acad. Sci. USA* **2014**, *111*, 8788–8790. [CrossRef] [PubMed]
22. Goolsby, R. On Cybersecurity, Crowdsourcing, and Social Cyber-Attack, 2013. Wilson Center. Available online: https://www.wilsoncenter.org/sites/default/files/127219170-On-Cybersecurity-Crowdsourcing-Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf (accessed on 1 May 2016).