Cyber-war:
A new chapter in international law development

Kamal Makili-Aliyev

Abstract

Cyber-warfare is no longer science fiction. It is quite real. With global infrastructure growing increasingly dependent on cyberspace and its networking systems, defense against cyber-attacks is already a worldwide concern. Unimaginable 20 years ago, states dependent on the networked world are trying to come to a consensus on the regulation of cyberspace. International law regulation of cyberspace is one of the key issues. Can states use force in response to cyber-attacks? Can a cyber-attack be so serious that it can trigger self-defense mechanisms via international law? Is it possible that future cyber-attacks could erupt into full scale physical wars? What are states' current attitudes towards cyber-warfare norms in international law? This article will illuminate these issues and several other important questions, analyze key aspects of international legal regulation of cyberspace and cyber-warfare, and present conclusions.

** Kamal Makili-Aliyev is Leading Research Fellow in the Center for Strategic Studies in Baku, Azerbaijan*

Today, international law is facing a new age of development in terms of *jus ad bellum*. More and more, terms like 'cyber-attack' or 'cyber-war' are already being used to define breaches of computer systems around the world at national level. At the same time, an ever-increasing number of such breaches demand legal coverage at both global and national levels. It seems that neither international law nor the legal systems of the majority of countries have been developed to address the current cyber security situation. The implications of such a backlog are hard to underestimate. Already, the threat posed by the growing number of what are now called 'cyber-attacks' extends beyond private or corporate entities to international peace and security.

Right now, there exists a variety of opinions on the threat of cyber-attacks and cyber-war. Former Director of National Intelligence Michael McConnell argues that "[t]he United States is fighting a cyber-war today, and we are losing. . . . As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking".[1] McConnell considers the defense of key cyber-infrastructures critical to state security. At the same time, some scholars believe that while cyber-espionage — stealing government and corporate secrets through infiltration of information systems — is a major challenge, the risks of major cyber-attacks are exaggerated.[2] Many experts say that terrorist or criminal groups also pose cyber-threats, but they also note that for now, the greatest potential for damage through cyber-attacks lies with a handful of countries.[3]

Not long ago, the London-based International Institute for Strategic Studies announced that the latest research on cyber-warfare indicates a growing consensus that future conflicts may feature the use of cyber-warfare to disable a country's infrastructure, meddle with internal military data, try to confuse a country's financial transactions, or accomplish any number of other potentially crippling acts.[4]

This confirms the view that the current situation creates a considerable number of new risks, and endangers international security. This article is concerned with the extent to which international law regulates cyber-capabilities in the modern world, and will address specifically the question of whether a cyber-attack can constitute an act of aggression - and if it does, does that justify a response that

1 . Mike McConnell, To Win the Cyber-War, Look to the Cold War, WASH. POST, Feb. 28, 2010, at B1.

2 . Seymour M. Hersh, The Online Threat, NEW YORKER, Nov. 1, 2010, at 44, 48.

3 . See CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 13 (2008), available at http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

4 . Press Release, John Chipman, Dir.-Gen. & Chief Exec., Int'l Inst. for Strategic Studies, Military Balance 2010—Press Statement (Feb. 3, 2010), available at http://www.iiss.org/publications/ military-balance/the-military-balance-2010/military-balance-2010-press-statement/.

involves the use of force? Additionally, this article strives to better understand contemporary relationships between international laws that regulate force, and cutting-edge technologies.

Use of force in international law and cyber-attacks:

The UN Charter is the starting point for legal regulation of the use of force. Its Article 2(4) provision rules that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations".[5] At the same time, Article 51 of the UN Charter states that: "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations".[6] Prohibition of use of force is quite strict, though despite debates on the actual possibility of military force usage in self-defense, it is universally accepted that Article 51 is the only exception to the rule of Article 2(4) of UN Charter. At the same time it is also generally accepted that the term "armed attack" is a much narrower notion than "threat or use of force".[7]

If we consider the definitions provided above, the questions of whether a cyber-attack can constitute a prohibited "use of force", and whether military force can be deployed as self-defense in return, become alarmingly clear. Because we are dealing with new technologies and the related terminology, interpretation of the aforementioned articles of the UN Charter become somewhat tricky.

On one hand we have the view of the majority in international law that Article 2(4) on the prohibition of force and the related Article 51 on the right to self-defense refer to military attacks and related hostilities.[8] That view is supported by the wording of Article 51: self-defense against "armed" attacks. Again, this norm also suggests that the drafters of the UN Charter understood "force" as a broader category than "armed attack". Nonetheless, the drafting history of the UN Charter as well as an analysis of the terminology used throughout the document in question demonstrates a strong intent on behalf of the drafting team to regulate armed force more strictly than any other method of coercion.[9]

On the other hand, however, there are also views that Article 2(4) should be interpreted more broadly, and that it prohibits coercion generally, armed force being only one (if the most evi-

5 . U.N. Charter art. 2, para. 4.

6 . Id. art. 51.

7 . See Albrecht Randelzhofer, Article 51, in 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 788, 796 (Bruno Simma ed., 2d ed. 2002).

8 . Bert V. A. Roling, The Ban on the Use of Force and the U.N. Charter, in THE CURRENT LEGAL REGULATION OF THE USE OF FORCE 3, 3 (A. Cassese ed., 1986).

9 . Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 COLUM. J. TRANSNAT'L L. 885, 905 (1999).

dent) method.[10] This approach is problematic in the sense that coercion can be legal, and indeed can constitute a reasonable element of international relations between many states.[11] But this interpretation has merit even if it is difficult to differentiate between legal and illegal coercion.

Of these two perspectives, the second one actually allows the interpretation of a cyber-attack as the "use of force" as meant by Article 2(4), and also justifies self-defense as a response to such an attack, in line with Article 51. The main issue here is focusing on the interpretation of UN Charter based on its intent rather than its text. Following that logic, offensive cyber-attack capabilities, such as inserting malicious computer systems codes to disable public or private information systems or functions that rely on them, have distinct similarities with use of military force, economic coercion, and subversion. Cyber-attacks also, of course, have unique characteristics. Such attacks evolve very quickly and in unpredictable ways.[12]

The U.S. Defense Department's analysis of the matter argues that: "If we focused on the means used, we might conclude that electronic signals imperceptible to human senses don't closely resemble bombs, bullets or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack than in its mechanism".[13] Basically, this report suggests that cyber-attacks can be considered equal to armed attacks, and thus the state can invoke the right to self-defense. These views of the U.S. government are reinforced by the statements given by officials.[14]

The situation as a whole gives rise to speculation that as states start to perceive cyber-threats as an integral part of their security policies, the questions of cyber-warfare and UN Charter provisions will become more and more important to the international community. At the same time it is not certain whether international law would demand the broader legal interpretation of the UN Charter, or whether new legal instruments would be adopted to deal with the cyber-attacks as they currently exist - bearing in mind their constant development and evolution.

10 . Ahmed M. Rifaat, International Aggression: A Study of the Legal Concept 120, 234 (1980).

11 . Alexander L. George, Coercive Diplomacy: Definition and Characteristics, in THE LIMITS OF COERCIVE DIPLOMACY 7, 7-11 (Alexander L. George & William E. Simons eds., 2d ed. 1994).

12 . Matthew C. Waxman, Cyber-Attacks And The Use Of Force: Back To The Future Of Article 2(4), THE YALE JOURNAL OF INTERNATIONAL LAW, Vol. 36: 421, 2011, p. 431.

13 . U.S. DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 18 (1999), available at http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf, reprinted in 76 INT'L L. STUD. 459, 483 (2002).

14 . Hillary Rodham Clinton, U.S. Sec'y of State, Remarks at the Newseum in Washington, D.C. (Jan. 21, 2010), available at http://www.state.gov/secretary/rm/2010/01/135519.htm; Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the S. Armed Services Comm., 111th Cong. 11-12 (Apr. 15, 2010), available at http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf.

The U.S. Defense Department's analysis of the matter argues that: "If we focused on the means used, we might conclude that electronic signals imperceptible to human senses don't closely resemble bombs, bullets or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack than in its mechanism".

The U.S. position is probably the closest to a consequence-driven interpretation of "force" or "armed attack" with respect to cyber-attacks, not only in terms of what it includes (i.e. what the UN Charter explicitly prohibits that would allow the invocation of self-defense rights), but also for what it excludes. Computer-based espionage, intelligence gathering, or even some preemptive cyber-operations or countermeasures designed to disable an adversary's threatening capabilities, for example, would generally not constitute prohibited force because these activities do not produce destructive consequences analogous to an actual (physical) military attack.[15]

Some legal experts have expressed views that for a cyber-attack to qualify as "force" or "armed attack", it must directly lead to "violent consequences."[16] Such consequences might include causing a major power system to explode by infiltrating and disrupting its computer control system, for instance. Such measures would constitute "force" or armed attack"; however causing the same system to just to shut down by the same means — even for a long time — probably would not. This position is more concerned with the mechanisms employed to produce harmful effects, and it implies that a state facing cyber-attacks could act in armed self-defense only against certain very specific attacks in cyberspace.

This position has been adopted by Pentagon in its new Cyber Strategy, in the main a product of the notion of "equivalence." If a cyber-attack produces the death, damage, destruction or high-level disruption that a traditional military attack would cause, then it would be a candidate for a "use of force" classification, which could merit self-defense. The Strategy has also prompted a debate over a range of sensitive issues not addressed by the Pentagon in its report, for example, whether the U.S. can ever be certain about an origin of the attack, and how to decide when computer sabotage is serious enough to constitute an act of war. These

15 Sean P. Kanuck, Information Warefare: New Challenges for Public International Law, 37 HARV. INT'L L.J. 272, 275-76 (1996).

16 Yoram Dinstein, Computer Network Attacks and Self-Defense, 76 INT'L L. STUD. 99, 103 (2002).

questions have already been disputed within the military.[17] One problem raised by such an approach is that "violent" damage can be significantly less serious than "non-violent" damage. This is clear when we consider, for example, the damage imposed by economic sanctions, compared with certain enforcement operations; or, for instance, a cyber-attack that takes down the power grid for an extended period, potentially leading to lead to public health problems and compromising public safety, despite the initial act being "non-violent". Despite these objections, the Pentagon's view is supported by some scholars.[18]

The Pentagon recognizes that civilian and military infrastructure has grown more dependent on the Internet. This motivates the military to formalize the Pentagon's cyber strategy. The realization that they have been slow to build up cyber-defenses prompted them to establish a new command last year, headed by the director of the National Security Agency. This new initiative is in charge of consolidating military network security and attack efforts. The Pentagon itself was shaken by the cyber-attack in 2008, a breach significant enough that the Chairman of the Joint Chiefs briefed then-President George W. Bush. Pentagon officials said they believed the attack originated in Russia, although they didn't say whether they believed the attacks were connected to the Russian government. Russia has denied any involvement.[19] This incident clearly shows the developments in the cyber-warfare situations around the world. There are other examples of serious cyber-attacks that will be discussed later in this paper.

While Article 2(4) of the UN Charter was never really deemed capable of entirely preventing armed collisions and hostilities without solid international backup sufficiently strong and independent to implement it, when looking at previous uses of the provisions of Article 2(4), it becomes evident that the provisions of Article 2(4) can both reduce the chances of aggression, and amend the form that aggressive actions take, by increasing the costs of certain actions. In any case, the Charter's normative principles set boundaries for measures taken by states to defend or advance their security interests by dictating procedures through which those measures are justified publicly and measured against international community expectations, which affect the costs (political, diplomatic, etc). Some scholars take the argument even further, claiming that norms governing the "use of force" exert significant internal pressure on state decision-making, especially among

17 Siobhan Gorman and Julian E. Barnes, Cyber Combat: Act of War. Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force, WALL STREET JOURNAL (May 31, 2011), available at http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

18 Walter Gary Sharp, Sr., CYBERSPACE AND THE USE OF FORCE 140 (1999).

19 See Gorman, supra note 17.

some types of states.[20]

Scholars studying the problem of legal regulation of cyber-attacks usually focus on the problems of identification and attribution: it is not always possible to discern quickly or accurately the perpetrator of an attack. The nature of digital information infrastructure facilitates anonymity, even allowing adversaries to route their attacks through computer systems belonging to other parties. In addition, the nature of forensics means that it may be very difficult to pin a case of penetration or disruption of a computer or information networks to the responsible party, even though forensic capabilities are generally improving, though not evenly across states. Even if individual perpetrators can be identified, it may be difficult to identify on whose behalf they are operating.

Scholars studying the problem of legal regulation of cyber-attacks usually focus on the problems of identification and attribution: it is not always possible to discern quickly or accurately the perpetrator of an attack.

This perception is shared by Pentagon Cyber Strategy critics. Gorman points out that: "[Strategy] will also spark a debate over a range of sensitive issues the Pentagon left unaddressed, including whether the U.S. can ever be certain about an attack's origin... [that] have already been a topic of dispute within the military".[21]

Though it seems only to be a technical issue, the issue of identifying the source of the attack also brings up large-scale jurisdictional problems. When cyber-attack occurs, it can affect a variety of transit computers all around the world and in many different countries. On the other hand, states are usually limited in their jurisdiction outside their sovereign borders. And even if the attack can be accurately traced to its source, there are problems with publicity. States are not usually in the habit of immediately acknowledging the breaches in their systems, because it might provoke discussion of their technical capabilities, revealing private information to their opponents or third parties. A relevant example is the aforementioned case where malicious software got into the Pentagon's classified and unclassified computer systems through a flash drive inserted into a military laptop. That happened in 2008, but the U.S. did not acknowledge "the most significant breach of US military computers ever" until almost two years later, and still there was nothing mentioned about the scale of the damage or if the sources of the cyber-attack

20 See Sean D. Murphy, The Doctrine of Preemptive Self-Defense, 50 VILL. L. REV. 699, 702-05 (2005); See also Thomas H. Lee, International Law, International Relations Theory, and Preemptive War: The Vitality of Sovereign Equality Today, 67 LAW & CONTEMP. PROBS. 147, 158 (2004).

21 See Gorman, supra note 17.

had been identified.[22]

There are also problems with the identification of the perpetrators and, as a result, with the enforcement of the law.[23] The basic thought here is that the ability to determine the ultimate perpetrator and sponsor of cyber-attacks may be crucial in taking effective defensive or deterrent actions, following a state's internal legal obligations, and justifying a state's external responses. At the same time, the level of certainty a state requires internally is usually different to the level of certainty that is needed to externally justify responses of such state.

Ultimately, the main thought remains that besides the specific challenges of regulating certain types of conflict, previous experience of interpreting the U.N. Charter illustrates important principles about the relationship between law and power, and that these principle are applicable to a discussion of cyber-capabilities. Competing interpretations of Articles 2(4) and 51 have always reflected distributions of power. The corollary of this is that efforts to revise legal boundaries and thresholds may have re-allocative effects on power by raising or lowering the costs of using resources and capabilities that are not equally apportioned.[24]

America's new "International Strategy for Cyberspace" and its international law implications:

The "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" (hereinafter Strategy) was released by the current U.S. Administration on May 16, 2011. President Obama's statement on the Strategy pointed out that this was "the first time that our Nation has laid out an approach that unifies our engagement with international partners on the full range of cyber issues." Building the rule of law through international norms and processes is considered crucial in maximizing the potential of cyberspace, and at the same time deterring any threats to its expanded use.[25]

The 1990s marked the beginning of widespread private, corporate and governmental use of Internet, and since then, the U.S. government has been trying to regulate the use of cyberspace and protect its users from harmful activities. The international growth of cyber-crimes was a direct result of increasing importance of cyberspace in social and economic spheres as well as in the political life.

22 William J. Lynn III, Defending a New Domain: The Pentagon's Cyberstrategy, FOREIGN AFF., Sept./Oct. 2010, at 97. See also Ellen Nakashima, Defense Official Discloses Cyberattack, WASH. POST, Aug. 25, 2010, at A3.

23 COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 10-11 (2009), at 252-253, 303.

24 See, Paul B. Stephan, Symmetry and Selectivity: What Happens in International Law When the World Changes, 10 CHI. J. INT'L L. 91 (2009); See also, Waxman, supra note 12, at 448.

25 White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011), available at http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

In 2008, a report release by the Center on Strategic and International Studies (CSIS) d report raised a number of concerns about the ineffectiveness of U.S. policies on protecting the Internet use and its users. The report explicitly stated that one of the most urgent national security problems for U.S. is its inability to protect cyberspace.[26] The current presidential administration began to revise its approach to cyberspace and concluded that the threats to cyberspace are right now one of the most difficult economic and national security issues that U.S. and its allies are facing.[27]

The current administration is not concentrating exclusively on cyberspace security. Secretary of State Hillary Clinton's speech on internet freedom in 2010 is a clear sign that the U.S. Administration is trying to introduce a normative perspective towards the Internet as a global political arena.

The current administration is not concentrating exclusively on cyberspace security. Secretary of State Hillary Clinton's speech on internet freedom in 2010 is a clear sign that the U.S. Administration is trying to introduce a normative perspective towards the Internet as a global political arena. Clinton said that U.S. advocates a single cyberspace (Internet) where all people have equal access to knowledge and ideas. She linked the achievement of this goal with the advance of freedoms of expression and worship, and freedom from fear and want.[28] Most analysts agree that that this idea of "cyber-freedom" became more popular in the course of democratic uprisings in certain Middle Eastern and North African countries (the so-called "Arab spring") in the first half of 2011, and that the U.S. used this opportunity to promote an ideology in connection with the possibilities new cyberspace technologies have created for mankind globally.

The New Strategy clearly incorporates the U.S.'s strategic approach towards cyberspace with economic, political and security elements of U.S. policy. The Strategy endeavors to develop and use the advances in economic, social and political areas as advantages for a world united by the Internet, as well as dealing with the dangers that restrict the value of cyberspace in terms of international relations and cooperation, communications and trade.

26 Center on Strategic and Int'l Studies [CSIS], Commission on Cybersecurity for the 44th Presidency, Securing Cyberspace for the 44th Presidency 11 (Dec. 2008), available at http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

27 White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure 1 (2009), available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

28 Secretary of State, Hillary Clinton, Remarks on Internet Freedom (Jan. 21, 2010), available at http://www.state.gov/secretary/rm/2010/01/135519.htm.

The Strategy reaffirms "fundamental freedoms, privacy and the free flow of information" as the main guiding principles for achieving the aforementioned goals, and states that while safeguarding cyberspace the commitment to these guiding principles shall not waver. The Strategy points out that commitment to the freedoms of expression and association is abiding, but does not come at the expense of public safety or the protection of citizens. It also declares that U.S. is committed to ensuring a balance between the protection of citizens and their interests, and privacy, by giving law enforcers appropriate investigative authority, while protecting individual rights through appropriate judicial review and oversight to ensure consistency with the rule of law. The Strategy also advances the notion that states do not, and should not have to choose between the free flow of information and the security of their network systems. Maintenance of the security of networks shall not hinder the free flow of information. The Strategy acknowledges that guiding principles are often characterized as incompatible with effective law enforcement, anonymity, the protection of children and secure infrastructure. In reality, however, good cyber security can enhance privacy, and effective law enforcement targeting widely-recognized illegal behavior can protect fundamental freedoms. The Strategy states that: "[t]he rule of law — a civil order in which fidelity to laws safeguards people and interests; brings stability to global markets; and holds malevolent actors to account internationally — both supports our national security and advances our common values."[29] The Strategy aims promote open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, it is necessary to build and sustain an environment in which norms of responsible behavior guide state actions, sustain partnerships, and support the rule of law in cyberspace.[30] Striving to attain that goal requires the United States to engage internationally in integrated efforts through diplomacy, defense, and development policies.[31] To reinforce such initiatives, the International Strategy defines U.S. government activities in that direction "across seven interdependent areas of activity, each demanding collaboration within... government, with international partners, and with the private sector." These areas of activity are:

1. Economy (promoting international standards and innovative open markets);
2. Protecting networks (enhancing security, reliability, and resilience);

29 See International Strategy, supra note 25, at 5.

30 Id., at 8.

31 Id., at 11-15.

3. Law enforcement (extending collaboration and the rule of law);
4. Military (preparing for 21st century security challenges);
5. Internet governance (promoting effective and inclusive structures);
6. International development (building capacity, security, and prosperity);
7. Internet freedom (supporting fundamental freedoms and privacy).[32]

Throughout, the Strategy stresses the need for the rule of law to govern cyberspace both domestically and internationally. In the text, the "rule of law" is described as "a civil order in which fidelity to laws safeguards people and interests; brings stability to global markets; and holds malevolent actors to account internationally."[33] It is clear that international law and legal processes are crucial to the Strategy's vision of openness, prosperity and security in the world of networking. The Strategy confirms that existing principles and norms of international law also apply in cyberspace, including respect for the fundamental civil and political rights of freedom of expression and association, privacy, and property; state responsibility to deny criminals safe haven; and the right to use force in individual or collective self-defense in response to armed attacks. What is particularly interesting is the Strategy's understanding of the right to self-defense explained as: "Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."[34]

What is particularly interesting is the Strategy's understanding of the right to self-defense explained as: "Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."

The Strategy also emphasizes that due to the unique features of networking technology, emerging cyber-specific norms require development and implementation, while existing international legal norms that operate in cyberspace require greater clarity of definition. Such norms include:

1. Global Interoperability (States should act within their authority to help ensure the end-to-end interoperability of an Internet accessible to all);
2. Network Stability (States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with inter-

32 *Id., at 17-24.*

33 *Id., at 5.*

34 *Id., at 10.*

nationally interconnected infrastructure);

3. Reliable Access (States should not arbitrarily deprive or disrupt individuals' access to the Internet or other networked technologies);
4. Multi-stakeholder Governance (Internet governance efforts must not be limited to governments, but should include all appropriate stakeholders);
5. Cybersecurity Due Diligence (States should recognize and act on their responsibility to protect information infrastructure and secure national systems from damage or misuse) [35]

While acknowledging the importance of the international law norms and principles, the Strategy also focuses on international cooperation and strengthening international partnerships that can build consensus around principles of responsible behavior in cyberspace, and the actions necessary to build a system of cyberspace stability.[36] One of the main problems with the Strategy is that it directly affects such principles of international law as respect for sovereignty and non-intervention in the domestic affairs of states, without discussing these principles. Thus the consensus building with countries that have the power to define how cyberspace functions (China, for example) may lead to agreement only on the superficial principles of "responsible behavior" in cyberspace, avoiding the consensus in areas like political and civil rights.

These negotiations are already underway, and it has been reported that the U.S. and China have been holding private talks on cyber-security for more than two years. Their informal discussions have already led to progress in terms of cooperation to combat Internet fraud, an urgent problem for both countries. At the same time, the talks appear to have revealed a wide gap between the United States and China over almost everything virtual: policing computer networks, moderating cyber warfare, even controlling information. "Digital attacks and cyber snooping on U.S. technology firms and government agencies including the Pentagon, many of them believed to have originated in or been routed through China, have pushed cyber-security up the list of thorny issues troubling Sino-American relations."[37]

Conclusion:

Cyber-wars are already a threat to international peace and security. It is evident from both the recent instances of cyber-attacks all around the globe and the reactions the attacks have received. Countries are now in the process of realizing that international law needs a push towards

35 Id.

36 Id., at 11.

37 Reuters, U.S. and China face vas divide in cyber issues (15 July 2011), available at http://bit.ly/roEGSc.

the regulation of the conduct of the states, should a full-scale cyber-war suddenly erupt.

Scholars are more focused on cyber-security studies than ever; the U.S. and China hold talks on cyber-security issues trying to reach to common grounds at least on basic aspects of cyberspace regulations; the U.S. International Strategy for Cyberspace is being published (soon to be followed by the Pentagon's Cyber Strategy). All of these are the first signs of activities aimed at bringing international regulation to cyberspace.

Due to the growing and expanding use of the Internet and cyberspace in the Caucasus region, the international importance of regulation of cyber-warfare issues should not be underestimated here. Technological advances and IT infrastructure development together with the growing arms industry means that research of cyber-warfare means and methods is urgently required. Given the lack of the international monitoring in this area, there is a risk of "cyber-weapons" production. Considering that many international armed conflicts are live in the region (though lacking active hostilities), there is a strong possibility that with time, parties to these conflicts may turn to cyber-warfare. And here international law will be crucial. Who will be in the position to use armed force? Who will be exercising self-defense? What about respect for sovereignty? How will issues surrounding the seriousness of the cyber-attack and the proportionality of use of force be dealt with?

All of the aforementioned questions will require answers. Though the U.S. International Strategy for Cyberspace recognizes the possibility of responding to a cyber-attack with armed force, this is the opinion of one state, and as the Strategy acknowledges, international law needs further clarification and extension of norms when it comes to cyberspace.

Hope remains for a productive and timely dialogue between states, which can produce a new chapter of international law to handle the cyber-warfare consensus.