THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 3 Article 4

9-2017

Legislative Requirements for Cyber Peacekeeping

Nikolay Akatyev
Horangi, nikolay.akatyev@gmail.com

Joshua I. James
Legal Informatics and Forensic Science Institute Hallym University, joshua.i.james@pm.me

Recommended Citation

Akatyev, Nikolay and James, Joshua I. (2017) "Legislative Requirements for Cyber Peacekeeping," *Journal of Digital Forensics, Security and Law*: Vol. 12 : No. 3 , Article 4.
DOI: https://doi.org/10.15394/jdfsl.2017.1447
Available at: https://commons.erau.edu/jdfsl/vol12/iss3/4

LEGISLATIVE REQUIREMENTS FOR CYBER PEACEKEEPING

Nikolay Akatyev[†] and Joshua I. James[‡]
[†]Horangi, Singapore
nikolay.akatyev@gmail.com

[‡]Legal Informatics and Forensic Science Institute
Hallym University
Chuncheon, South Korea 24252
joshua@cybercrimetech.com

ABSTRACT

Cyber Peacekeeping strives for the prevention, mitigation and cessation of cyber and physical conflicts. The creation of a Cyber Peacekeeping organization, however, has major legal and political implications. In this work, we review current international legislation applicable for functions of Cyber Peacekeeping. Specifically, we analyze prominent works which contribute to definitions, law and ethics regulating cyber conflicts from the perspective of the creation of a CPK organization. Legislative and terminological foundations are analyzed and adopted from current practice. Further, this work analyzes guiding principles of global organizations such as ITU IMPACT, INTERPOL and regional organizations such as NATO and the Shanghai Cooperation Organisation to identify strengths and weaknesses of such international cooperation, and how Cyber Peacekeeping could fill current gaps relating to cyber conflict response.

Keywords: cyber peacekeeping, international security, cyber conflict, international relations, critical infrastructure, cyber terrorism, cyber war, conflict escalation, cyberspace

1. INTRODUCTION

Previous work introduced the concept and structure of Cyber Peacekeeping (Akatyev & James, 2015). The main goal of Cyber Peacekeeping (CPK) is to promote online safety and security, which assists in both physical and cyber conflict cessation, and helps protect cyber civilians from becoming either victims or participants in cyber conflicts. Protection and prevention is provided through pre- and post-conflict monitoring, cleanup and capacity building, as well as response and coordination activities during conflicts. While past work defined CPK organizational structure and basic functions, little consideration was given to the legislative requirements for such an organization. This work will analyze legislative requirements of current peacekeeping operations, and give recommendations about legislative and political cooperation necessary to create useful Cyber Peacekeeping organizations.

One of the first cyber attacks that allegedly happened in 1982 involved sabotaged software in a Trans-Siberian gas pipeline that lead to an explosion (Reed, 2007). Even with some precedent, it wasn't until StuxNet in 2010 that complex, targeted attacks with military - rather than financial - motivations began to be considered a serious threat (Langner, 2011). At the same time, the Arab Spring was showing the power, for better or worse, of social media, cyber activism and hacktivism (Karatzogianni, 2013). Since then, there has been an increase in the use

of information warfare, and in some cases re-purposing cyber weapons, by actors involved in both digital and physical conflicts (Farwell, 2014). This situation eventually led to an increased focus on developing 'cyber warriors' as a bigger part of official military actions (Eom, Kim, Kim, & Chung, 2012; Gjelten, 2013; Solce, 2008). This increased potential for direct cyber conflicts as well as the escalation of online or offline conflicts through the use of information warfare in cyberspace has consequences for not only the main actors, but also online bystanders whose right to safety and justice should be considered and protected (Denning, 2008).

History of Company

This work contributes to the discussion of cyber warfare prevention, mitigation and cessation through the creation of peacekeeping powers that can be applied to cyberspace. This is one of the first works to propose legislative considerations for an international organization dedicated to peacekeeping activities in cyberspace related to physical conflict. However, finding a common ground among not only states but also with for-profit and nonprofit private organizations shows significant challenges. This work analyzes existing and proposed norms and guiding principles of existing organizations from the point of CPK creation and governing.

Cyber Peacekeeping

Cyber Peacekeeping seeks to prevent and mitigate cyber and physical conflicts before the conflict escalates. Further, CPK works towards conflict cessation during periods of conflict. These goals are achieved through cyber conflict prevention, mitigation, post-conflict containment and rehabilitation services. Two specific implementations of mitigation services previously proposed include the concept of a Cyberspace Safe Layer (CSL), and an Information Clearinghouse (ICH). The CSL addresses the need to define and protect critical cyber infrastructure and help delineate unethical targets in conflicts (Schmitt, 2013). The ICH helps in the tempering of rumor and bias on social networks that is likely to lead to the escalation of digital and/or physical conflicts, and potential recruitment of unaffiliated actors.

The creation of a Cyber Peacekeeping organization, however, has major legal and political implications. The legal implications of CPK can be considered by examining current incidents of cyber conflict. A brief example is the Syrian war that has included elements of cyber conflict (Lee, 2016). Attacks on cyber assets, tracking of people and borderless propaganda directly led to the escalation of physical conflict. In this case study, the implementation of the CPK Information Clearinghouse may be a first step in minimizing escalation through online propaganda. However, from a legal point of view, all stakeholders should agree on what information can be considered propaganda, and what information is protected freedom of speech. Unfortunately, consensus between stakeholder is not easy, as the West is traditionally leaning toward holistic freedom of speech; supporting dissidents in China and Russia, whereas the East, represented by the Shanghai Cooperation Organization, would see a threat to their political systems. Thoroughly studying the critical terminology foundations from the EastWest Institute and other related works from each perspective, we propose a more neutral approach that may be accepted by both sides for the mitigation of the conflict in the specific case of Syria.

1.1 Cyber Peacekeeping Structure

To carry out its mission, we define goals, roles and functions for Cyber Peacekeeping as shown in Figure 1 (Akatyev & James, 2015). Each role of Cyber Peacekeeping can contribute to the

safety and security of cyberspace at all three stages of a conflict: no conflict, during conflict, after conflict. For example, CPK as a guardian will monitor potential threats when there is no conflict. During conflict, it will stop the spread of cyber-attacks and involved cyber weapons responding with 'defensive counterattacks' as a last resort for "self-defense or defense of the mandate" ("Principles of UN peacekeeping," n.d.). After conflict CPK as a guardian will lead cleanup activities related to distribution and alteration of cyber weapons. Figure 1 shows relations among roles and their functions for different stages of a conflict depicted by different types of lines: solid (guardian), dot (mediator), dash (coordinator), dash-dot (builder).

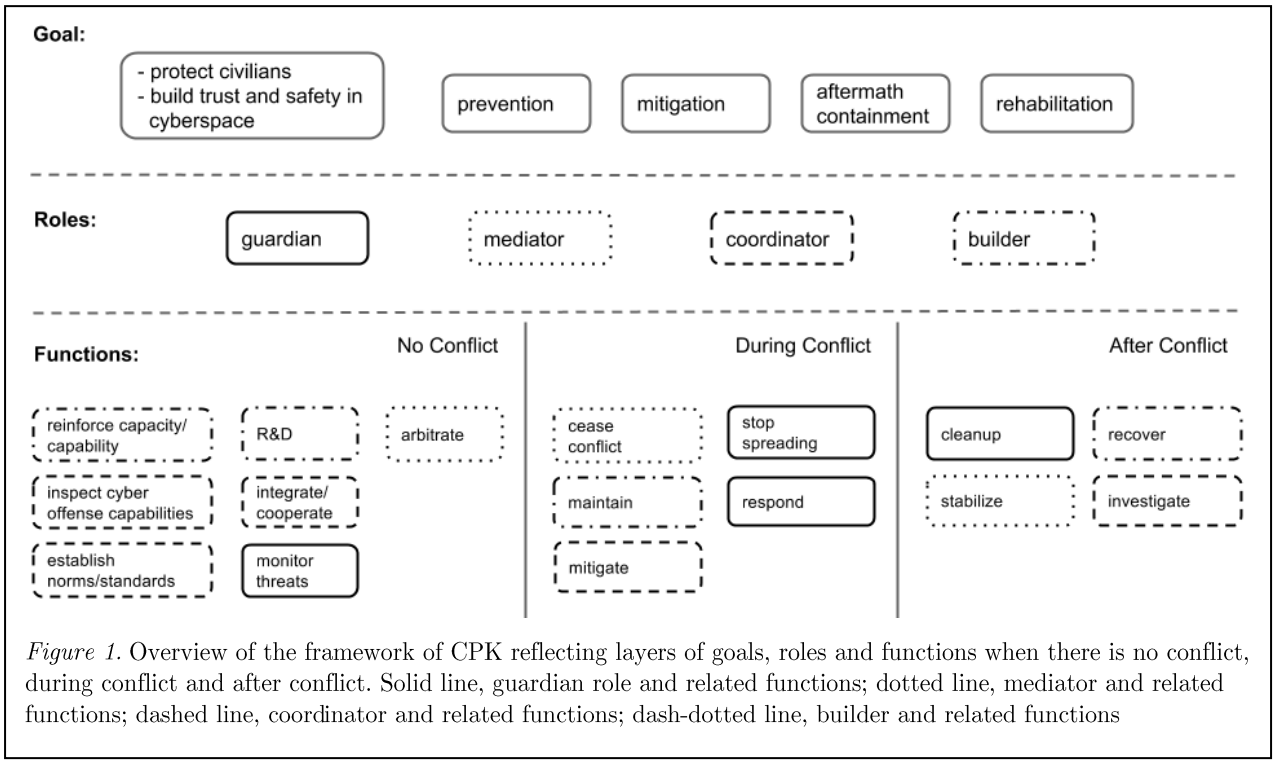

Figure 1. Overview of the framework of CPK reflecting layers of goals, roles and functions when there is no conflict, during conflict and after conflict. Solid line, guardian role and related functions; dotted line, mediator and related functions; dashed line, coordinator and related functions; dash-dotted line, builder and related functions

The goals of Cyber Peacekeeping are defined as:

1. Protect civilians
    a. The main goal of CPK is the protection of civilians. CPK must be impartial to any State independent of contributions.
2. Increase trust and security in cyberspace
    a. Through conflict prevention, mitigation and rehabilitation tasks, trust in cyberspace can be maintained and security increased.
3. Prevention
    a. Focuses on preparation for potential attacks, and preventing cyber conflict escalation when conflicts begin
4. Mitigation
    a. Focuses on containing conflicts and minimizing damage to infrastructure and civilians
5. Aftermath Containment
    a. Focuses on containment of tools and information that may be re-purposed or reused in other

conflicts, as well as using collected information for prevention

6. Rehabilitation
    a. Focuses on rebuilding infrastructure, security and trust post-conflict

1.2 Legislation for Cyber Peacekeeping Services

Based on these goals, CPK provides a number of services before, during and after conflicts. Each 'role' has a specific set of functions or services that are provided and are designed to complement each other. Very basically, these services fall into three broad categories; capacity building, maintenance and security, and recovery. The majority of Cyber Peacekeeping services do not require special legislation. For example, capacity building in the form of technical training can take place without the need for international legislation. Training and similar capacity building services could take place simply by invitation and agreement. Further, there is no need for international legislation regarding the research and policy recommendations put forward by CPK services, save for the ability to access potentially classified government data. However, such agreements could be made on a per-case basis. Cyber Peacekeeping, as proposed, does not encroach on the sovereignty of any member organizations. Much like INTERPOL, who has no authority to enforce law in any jurisdiction without prior permission, CPK too would have capacity for certain types of investigations, but would lack authority to carry out such functions without local permission. The two most invasive services that could be considered to encroach on the jurisdiction of states would be the Cyberspace Safe Layer and the Information Clearinghouse. The latter of which would not require cooperation from a government, but would greatly benefit from international cooperation. For this reason, we will focus on the legal requirements necessary to effectively implement these services.

1.2.1 Cyberspace Safe Layer

The Cyberspace Safe Layer is the pre-identified, minimally-required critical infrastructure necessary for civilian safety. Prior research describes the necessity to protect critical infrastructure (Das, Kant, & Zhang, 2012); however, there is no global consensus on the definition what constitutes critical infrastructure. The CPK together with the international community and individual States should attempt to define minimal critical infrastructure required for civilian safety. The Cyberspace Safe Layer then becomes the focus of CPK when conflicts arise in the country or region. Before conflict, the CPK would provide services to help secure identified critical infrastructure.

1.2.2 Information Clearinghouse

Another equally important part of conflict de-escalation is the management of an information clearinghouse that helps to identify verified and unverified information, and distribute this information to potential actors, such as citizens that may attempt to join physical conflict based on false information. While there are many real-world examples of propaganda being used to sway opinion, such propaganda online represents a direct threat of escalation of a cyber conflict into physical violence. The information clearinghouse is primarily focused on conflict de-escalation through information sharing.

2. CURRENT STATE OF CYBER CONFLICT RESPONSE

To determine the legal requirements for Cyber Peacekeeping, we selected critical terminology foundations from the EastWest Institute

(Godwin III, Kulpin, Rauscher, & Yaschenko, 2014), Tallinn Manual (Schmitt, 2013), OECD Security Guidelines (OECD Guidelines for the Security of Information Sy, 2002) and the EU Convention on Cybercrime (European Council, 2001), among others. Further, this work analyzes guiding principles and mandates of global organizations such as ITU IMPACT, INTERPOL and regional organizations such as NATO and the Shanghai Cooperation Organisation (SCO) to identify strengths and weaknesses of such international cooperation, and how CPK could fill current gaps relating to cyber conflict response, and the legal requirements, if any to fill these gaps.

2.1 Cyber Norms

Cyber Norms are behaviors that are considered acceptable to states in cyberspace. Defining norms of behavior give a guide to acceptable and unacceptable actions in cyberspace, as well as potential consequences. Of course, just as there are many cultures, so too are there many perspectives about what are acceptable behaviors that make agreement difficult. There is, however, motivation to agree on cyber norms.

> *The main goals for agreeing on norms are believed to include increased predictability, trust and stability in the use of ICTs, hopefully steering states clear of possible conflict due to misunderstandings. Additionally, norms are seen as guiding principles for shaping domestic and foreign policy as well as a basis for forging international partnerships.* (Osula & Rõigas, 2016)

As described, clearly defined cyber norms can help to build relationships based on expected behavior and avoid misunderstandings. Much like cultural interactions, an action can have a positive or negative interpretation based on the observer's perception.

Experts with the United Nations identified a set of voluntary non-binding norms for responsible behavior and confidence-building measures (United Nations, 2015a). Notably, that experts from two polar systems (the "Western view" and the "Eastern view") participated in the work of the group and accepted concerns of both parties, such as the importance of critical infrastructure and freedom of speech on the Internet as protected by Human Rights council resolutions, as well as cooperation against terrorist threats. This report also incorporated views suggested by members of the SCO to the UN. The experts recognized the applicability of the UN Charter in cyberspace.

The United States defined its preferred cyberspace norms - Internet openness, security, liberty, free speech, and with minimal government oversight and surveillance - in its 2011 International Strategy for Cyberspace (United States White House, 2011). Recognition that international law applies to state activity in cyberspace and that human rights protections that apply offline also apply online (Farrell, 2015). The US promotes soft norms to ensure predictable behavior by all states since the US infrastructure is vulnerable to cyberattacks and software always has subtle weaknesses; deterrence is not effective; treaties and checking compliance is not easy.

The West supports the application of existing international norms into cyberspace (Osula & Rõigas, 2016). China and Russia partially agree with this view but mostly they promote the development of new norms. China and Russia worry about sovereignty in cyberspace following a collectivist approach to cybersecurity.

Cyber Norms are still being negotiated (Hua, 2016; Kaljurand, 2015; Korzak, 2015; "NEWSLETTER," 2014; Segal, 2011), mostly from an Eastern/Western perspective driven by the SCO, NATO and related countries. Even

terminology needs to be defined and agreed on (Schmitt & Vihul, 2014). Progress is being made, and cyber norms will play a great role in cyber security in the future. Developing norms will be of great interest to CPK as they define normal and abnormal behaviors and potential consequences.

2.2 Critical Terminology

As discussed, agreement on terminology is important for building relationships and avoiding misunderstandings (similar to behavioral norms). Various organizations have proposed terminology with members and related countries generally accepting many terms. Ultimately, definitions come down to the accepted concepts by each organization. For example, two polar systems of the West (represented by NATO) and the East (represented by SCO) have orthogonal views to definitions of critical infrastructure and information. The West views cyberspace purely as computer networks while the East includes other means of transmission of the information in the concept of cyberspace (Godwin III, Kulpin, Rauscher, & Yaschenko, 2014). The information itself is also viewed differently by the West and the East where former supports any form of the information for the sake of the freedom of the speech as the East sees dangers to states' stability and sovereignty in some information which come from dissidents.

Russia - a major part of the SCO - uses the term 'information security,' which is broader than cyber-security (*Information Security Doctrine of the Russian Federation*, 2000). Russia recognizes a broader scope of threats in the information space and modifies its legislation tightening against information espionage and terrorism. The fourth component of the Russian information security doctrine includes the protection of information resources from unauthorized access, and the security of information and telecommunications systems that are already deployed and that are being established on the territory of Russia. Russia distinguishes between external and internal threats. According to the doctrine mentioned above, external threats include: the activities of foreign countries directed against Russian information interests, the intensification of international competition in information technology, the activities of international terrorist organizations, and the development of information espionage and warfare. The amendment to the criminal law deleted an earlier clause that criminalized "causing damage to computers and computer networks," making the prosecution of organizers of denial of service attacks harder. This attitude also affects the SCOs definitions and approaches to information security.

The EastWest Institute (EWI) developed critical terminology research to help determine whether or not a certain cyber action would result in intensified or violent escalation (Godwin III, Kulpin, Rauscher, & Yaschenko, 2014). This research is useful when attempting to find a common ground for the definition of critical infrastructure and the perception differences between the West (represented by the United States) and the East (represented by Russia). While concept mappings and agreements are useful, terms proposed by the EWI are merely recommendations for implementation at the state and regional levels.

The Organisation for Economic Cooperation and Development (OECD) has also defined terms such as 'critical infrastructure' and the role of member countries in protecting their systems (for economic purposes) (Gordon & Dion, 2008; OECD Guidelines for the Security of Information Sy, 2002). The OECD has more power to enforce a standardization of terms within member countries, but tends to take a more general approach to definitions.

As was shown, many organizations are attempting to define terminology (and promote

their particular conceptualizations); however, the groups definitions rarely align, and often conflict with each other. As can be seen with the EWI terms, discussion and conceptual mappings will be required as long as regional organizations work in isolation.

When working together, the American and Russian experts defined 'Critical Information Space' as the aggregate of elements of information space that are identified as essential by a national government or by international agreements (Godwin III, Kulpin, Rauscher, & Yaschenko, 2014). The experts also agreed on the term 'Critical Cyberspace;' cyber infrastructure and cyber services that are vital to the preservation of public safety, economic stability, national security and international stability. The concepts of Critical Information Space and Critical Cyberspace, as defined, can be a foundation for the Cyber Peacekeeping *Cyberspace Safe Layer*, where countries with various interests can agree that these concepts exist, and according to the definition, should be protected. CPK can work with such states to elaborate on the details of the Critical Information Space and related definitions from the perspective of all of its member countries.

The concept of a CPK *Information Clearinghouse* can follow from the agreement of the American and Russian experts concerning censorship. The censorship resolution came about when both sides agreed to move forward by (i) acknowledging the broader scope of "information," (ii) recognizing that "cyber" was a subset of this larger scope, and (iii) focusing on "cyber" because it is the area that required the most attention (Godwin III, Kulpin, Rauscher, & Yaschenko, 2014). CPK should not - and likely could not - directly censor information. The Information Clearinghouse, however, does seek to reduce the effectiveness of propaganda. Such efforts themselves may be seen as an effort to undermine current government powers. More discussion about "information," censorship and anti-propaganda approaches must be discussed. Though initially both the American and the Russian experts agreed to focus on "cyber," for the implementation of ICH, the CPK will foster further discussions about "information" and will clearly define which information from which actors can *escalate a cyber conflict*.

2.3 Jurisdiction

A great concern when dealing with cyberspace is the issue of jurisdiction and preservation of sovereignty (Osula & Rõigas, 2016). When considering CPK capabilities, some functions may directly conflict with efforts of local governments. Since CPK may provide resources outside of a country's jurisdiction that conflicts with their perceived sovereignty (or undermines their local authority) discussion is needed concerning how CPK can provide appropriate 'fact checking' without undue influence or retaliation when political conflicts occur.

There are generally two views concerning jurisdiction: the Exceptionalist vs the Sovereigntist (Watts, 2015). According to the Sovereigntist view, cyberspace, while novel with respect to the conditions that informed the creation of most existing treaties and customs, remains fully subject to international law. The Sovereigntist view continues to recognise sovereign states as both the stewards and subjects of international law in cyberspace. The Exceptionalist view, on the other hand, sees cyberspace as completely separate from territory, and thus current international legislation based on political borders does not apply.

As Levin, Goodrick, and Ilkina (2014) noted, since cyberspace is, in essence, a nexus of networks of computers that are physically located in many different countries and legal jurisdictions, no one country can dictate or control interactions in cyberspace. So, he concludes that countries therefore attempt to

enter into international agreements, either bilateral or multilateral, in an effort to regulate cyberspace and coordinate cyber-security, but these attempts are often guided by other interests and affiliations, which do not always correspond with the most effective responses to cybercrime. But still this tendency for international cooperation is a potential for CPK.

Experts with the United Nations agreed that "the most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State" (United Nations, 2015a). These attacks are not only devastating for States, but may be lethal for civilians. That's why it is not only under jurisdiction of an individual state but must be protected by international means especially as a strike can come from anywhere in the borderless cyberspace.

CPK must respect sovereignty of states; however, cyberspace is often defined as a borderless realm. So CPK should work with NATO, SCO, the UN and others to identify terms and conditions of sovereignty in the cyberspace. Such terms cannot be "Eastern" or "Western" concepts, but agreed at a global level. As identified in research by Erskine and Carr (2016), the challenge of ambiguous agents exists in the cyberspace. Addressing the question of the sovereignty, the international cyber norms must consider who are agents which conduct or receive a cyber act.

Main causes of cyber conflicts may be ambiguous agents or proxy actors in cyberspace ("Co-Chairs' Summary Report," 2012) which make attribution difficult; hence direct response by states may escalate a conflict attacking a wrong source of a threat. In order to prevent or mitigate a cyber conflict CPK will engage with ambiguous agents and proxy actors without breaking a condition of the sovereignty as defined through multi-stakeholder agreements. In such cases as described, CPK can react quickly and prevent incidents from escalating. In cases of complaints from states about the sovereignty violations, it would mean that states implicitly accept responsibility for wrongful agents (James, 2013), leading to political challenges for non-compliance.

2.4 Organization Mandates and Authority

To better understand what organizations could host Cyber Peacekeeping functions, or the entire structure, an understanding of current organization mandates is necessary.

UN Peacekeeping Operations are based on the normative framework of the Charter of the United Nations, Human Rights, International Humanitarian Law and Security Council Mandates (United Nations, 2008). Most member nations agreed to Peacekeeping efforts and collaborate for Peacekeeping Operations (PKO) recognizing threat and destructive consequences of a global war. Though the UN PKO revealed many challenges for such collaborations, they provide a solid case when nations with different cultures and views unite for the sake of a global benefit.

The International Telecommunication Union (ITU) launched the in International Multilateral Partnership Against Cyber Threats (IMPACT) as part of its structured approach in the fight against cybercrime, which includes legal measures, technical and procedural measures, organizational structures, international cooperation and capacity building. ITU IMPACT is an active member dealing with international cooperation activities. IMPACT engages with members for training and skills development, CIRT implementation, cyber drills, global response centre and child online protection ("IMPACT- International Multilateral Partnership Against Cyber Threats," 2016). IMPACT is the largest international public-private cyber security alliance and in summary it focuses on early

warning systems and developing a global secure electronic collaboration platform for incident response and threat mitigation. But the biggest challenge is that major cyber powers like the US, Russia, Japan and S. Korea do not participate in the organization. Another weakness of the organization is that it doesn't engage with threats directly but provides trainings and information sharing mostly for businesses.

We did not succeed in finding any documented governing principles or charters of this organization.

INTERPOL recognizes the global issue of cybercrime and possesses a unique level of access to the global network of national law enforcement ("INTERPOL," 2016). However, INTERPOL's mandate allows only consulting and information sharing roles with national Law Enforcement. It has no operational powers, and does not officially engage in discussion of international policies and norms for the cyberspace. INTERPOL is regulated by its constitution to which members of the organization are legally bound. These members are obligated to provide INTERPOL seconded personnel for activities on their own territories. Members of the organization contribute personnel and funding.

NATO recognized the threat of cyber-attacks after an incident in Estonia in 2007. That stimulated the alliance to declare that the cyber-attack would lead to invocation of Article 5 of the joint armed response (Osula & Rõigas, 2016). Also, NATO established The NATO Cooperative Cyber Defence Centre of Excellence and contributed to the research of the law of cyber warfare through the publication of the Tallinn manual (Schmitt, 2013). The Tallinn manual causes a concern that it discusses cases when States can respond to cyber-attacks with armed means in the cyber or physical space. That would lead to the escalation of conflicts.

Another regional organization, the Shanghai Cooperation Organization (SCO) led by Russia and China, is viewed as an organization with opposite views to NATO promoting new governance for the cyberspace. SCO supports the leading role of the UN, sovereignty of the state and control of 'inflaming information.' But the West accuses SCO in limiting the freedom of speech on the Internet (Osula & Rõigas, 2016). Since 2015, SCO extended its mandate for the cooperation in security including cybersecurity and economics. The members conduct military drills (Albert, 2009). Also, the experts from the member countries proposed the international conduct of behavior in the cyberspace as a letter to the UN (United Nations, 2015b).

Each of the discussed organizations contributes to the establishment of legislative principles of CPK. Though ITU IMPACT did not produce any documentation, it helps to initiate norms of international cooperation in the cyberspace which is an important start for the global approach of CPK. INTERPOL provides a solid reference for governing, structural and administrative principles of CPK. NATO helps understand how coalitions of States would react to cyber-attacks. And working with SCO's vision of a role for a global organization like the UN, CPK can establish its activities and broad its jurisdiction.

Presently, UN Peacekeeping Operations do not address problems in cyberspace and cannot be directly mapped to the cyberspace operations keeping in mind its current failures and challenges. The UN started considering the problem of peacekeeping in cyberspace with the recent introduction of the 'Digital Blue Helmets' program (United Nations, 2016). Presently, it appears as though the United Nations is best suited for housing Cyber Peacekeeping in a structure similar to traditional peacekeeping with guidance from discussed organizations.

2.5 Current Gaps in Cyber Peacekeeping Efforts

Governments attempting to build or affect cyber norms by themselves will have a difficult time in getting a general consensus globally. For example, the Snowden disclosure undermined the efforts of the US in building cyber norms (Farrell, 2015). A broader approach based on multi-country input and agreements is necessary.

As discussed, NATO and SCO are two major organizations which build capabilities in the cyberspace. But they approach and view the problem of the security in the cyberspace from different sides. ITU IMPACT achieved successful public-private partnerships, and conducts diverse activities including information sharing, monitoring of threats and capacity building, but current consumers of ITU IMPACT services are private companies. Though ITU IMPACT unified many countries, major players in cyberspace, such as the USA, China, Russia, S. Korea and Japan, didn't join the initiative.

The main gaps we observe that affect cyber peacekeeping is a concerted effort at an inclusive definition and strategy for conducting cyber peacekeeping operations. Initial cyber peacekeeping efforts should be focused on network building similar to ITU IMPACT, but with more country buy-in. It should also be focused on mapping concepts of existing definitions from different cultures as a starting point of communication between stakeholders.

A major gap that no organization has thoroughly addressed, is what cyber peacekeeping would do. The closest is the United Nations 'Digital Blue Helmets' that appear to focus on Dark Web and critical infrastructure issues (United Nations, 2016).

2.6 Current State of Support for Cyber Peacekeeping

Support for Cyber Peacekeeping is similar for support for traditional Peacekeeping efforts. Countries generally understand that conflict escalation and war is not desirable, and Peacekeeping can help reduce this risk ("Principles of UN peacekeeping," 2008). Cyber Norms and Terms have been defined at least regionally, with concepts being mapped through the efforts of organizations such as the EastWest Institute. Areas of contention exist, such as issues of censorship and online jurisdiction, that would hamper some CPK efforts. However, most CPK functions, as previously defined, would only require member state agreements and the approval of an oversight committee, such as the UN Security Council. Currently, only the United Nations has a mandate that could be considered to cover all CPK functions, but other organizations could also support specific functions within their legal remit.

Overall, Cyber Peacekeeping is legally practical. Organizational structures and technologies exist that can support some or all of the defined CPK functions. Issues of support arise when attempting to define specific aspects of CPK functions globally. Here, regional differences would likely oppose some the practical or conceptual objectives of CPK. In such a case, a model of cooperation similar to the EWI may be a starting point for cooperation and collaboration with member states.

3. FUTURE REQUIREMENTS OF CYBER PEACEKEEPING

Cyber Peacekeeping has a number of requirements to be practical and useful in the future. First, CPK should be based on the concept of cyber norms. To be effective globally, regionally-accepted cyber norms will need to be agreed upon (formally or informally) with the

majority of stakeholders. These cyber norms may then be used as a - less biased - baseline of acceptable behavior in cyberspace. Norms will only develop full legitimacy if they are associated with independent structures that evaluate them, debate them, and assess whether different actors are living up to them (Farrell, 2015).

Next, stakeholders need to agree on the concept of *Cyber Peacekeeping Operations*. In prior works, we described what some of the "operations" may look like (Akatyev & James, 2015), but our model most likely goes beyond what some member countries are willing to accept as peacekeeping operations, especially if their authority is somehow affected. In the case that a member is unwilling to support an operation, we are again presented with the issue that such an operation could take place outside of the opposing member's jurisdiction.

Similarly, future requirements (assuming our defined structure) include a chain of decision making and organizational practices. For example, what organizations will provide certain CPK services? When will CPK functions be available? When do we consider an online event a 'conflict', and which CPK functions should be available? Most importantly, what oversight body gets to make decisions about what 'state' CPK is currently in, in regards to particular online events.

3.1 Formal Requirements

As we have seen, the formal requirements for establishing Cyber Peacekeeping are minimal based on our current model. CPK does not have operational authority within member states, and thus does not need additional legal frameworks for any of its main functions. Though future development of a legally-binding collaboration based on a similar model to INTERPOL would be likely necessary for CPK to be effective as threats of cyber conflicts grow.

To support Cyber Peacekeeping functions, member states do need formally accepted terms, definitions and concepts that CPK works in. These include clearly distinguished language differentiating 'freedom of speech,' 'propaganda' and 'inflammatory information.'

It also includes a formal agreement on the protection of critical infrastructure (as defined in the critical terminology) by CPK according to the protection of civilians in International Humanitarian Law.

As the UN experts agreed about the applicability of the UN Charter in the cyberspace, States would need to formalize how the UN Charter exactly maps to different activities in the cyberspace. The States would need to work on clear descriptions of Peace, Breaches of the Peace and Acts of Aggression in cyberspace that CPK can rely on them during their operations.

A formal agreement would likely be required specifying the CPK governance structure, and especially the terms by which CPK could operate in conflict and non-conflict areas in cyberspace. Here member states would attempt to add a clause prohibiting CPK features from interfering with their local authority, which, if left as a general clause, could be used to deny CPK functions when authoritative governments are intentionally causing harm to their citizens (i.e. Syria [Amnesty International, 2016]); however, as we argued previously, the unique properties of the cyberspace will require rapid, executive actions by CPK across multiple 'jurisdictions' in cyberspace. So, the minimal but clear and essential agreement about responsibilities and authorities of CPK would be necessary at least in terms of the *Cyberspace Safe Layer*. Whether these agreements must be made through formal or informal processes depends on the attitudes related to sovereignty in cyberspace, and what powers are ultimately requested.

3.2 Informal Requirements

While formal requirements mostly relate to organization and oversight, informal requirements deal more with the practice of Cyber Peacekeeping. Specifically, the establishment, promotion (and potentially enforcement) of cyber norms. These cyber norms will be the basis for CPK operations.

After cyber norms (and formal agreement of terms), informal agreements will need to be established between CPK and individual member countries regarding services and access. For example, one function of CPK is to help secure, support and maintain critical infrastructure. First the scope of critical infrastructure would need to be formally defined, and informal agreements would need to be made with each member country regarding *how* CPK would help protect their infrastructure. Some members may allow full access to ensure CPK can properly maintain and monitor security, where other members would prefer CPK to be only an outside monitoring organization.

Informal requirements mostly deal with CPK member country agreements and permission to interact internally and externally to the member country. The conditions for that support, and the requirements member countries must meet to continue to receive such support from the CPK.

An essential part of the establishment of cyber norms is 'confidence building.' CPK would work with States, global and regional organizations in order to establish understanding among different groups with their own values and to promote best practices of 'appropriate' behaviour in cyberspace. The culture of training and information sharing already exists. Some groups also run anti-cyber terrorist operations and share technologies (Goldman, 2016; O'Connell, 2016). CPK will endorse these activities and facilitate their globalization to meet the goal of digital and traditional conflict prevention, mitigation and cessation.

4. CONCLUSIONS

There is currently a need for an organization or organizations to have broader cyber peacekeeping powers, but establishing peacekeeping powers online is fraught with political conflict and sovereignty issues. At the same time, Internet penetration in many countries is still relatively low, and cyberspace is not a common part of most people's lives. Under such circumstances, it is difficult for many countries to see the need for Cyber Peacekeeping. Unlike the immediately observable actions of traditional peacekeepers, the abstract concept of peacekeeping in cyberspace is not immediately observable and understandable to many. This is further complicated by the state of governance in cyberspace. Cyber norms and critical terminology are currently being discussed and developed, but a considerable amount of work remains to be done. Current organizations are focusing on offline conflict resolution measures, with some private organizations taking over some aspects of cyber peacekeeping through (and only on) their own platforms. There are many gaps between organizations that can contribute to cyber peacekeeping efforts. What is needed is a defined concept of Cyber Peacekeeping that is supported by many governments similar to traditional Peacekeeping. We are seeing ad-hoc cyber peacekeeping taking place, but a unified, directed effort is necessary for physical and digital conflict prevention and cessation in the future. The requirements for such a concept are all conceptual; definitions, legislation and agreements. The technical capabilities already exist. It is now up to governments to strive for cyber peace the way they work towards physical peace.

REFERENCES

Akatyev, N., & James, J. I. (2015). Cyber Peacekeeping. In Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST (Vol. 157, pp. 126–139). http://doi.org/10.1007/978-3-319-25512-5_10

Albert, E. (2009, March). The Shanghai Cooperation Organization. Retrieved September 15, 2016, from http://www.cfr.org/china/shanghai-cooperation-organization/p10883

Amnesty International. (2016, March). Syrian and Russian forces targeting hospitals as a strategy of war. Retrieved September 15, 2016, from https://www.amnesty.org/en/press-releases/2016/03/syrian-and-russian-forces-targeting-hospitals-as-a-strategy-of-war/

Co-Chairs' Summary Report. (2012) (p. ASEAN Regional Forum). Hoi An, Quang Nam, Viet Nam: ASEAN Regional Forum. Retrieved from http://aseanregionalforum.asean.org/files/library/ARF Chairman%27s Statements and Reports/The Nineteenth ASEAN Regional Forum, 2011-2012/10 - Co-Chairs Summary Report - ARF Workshop on Proxy Actors in Cyberspace, Quang Nam.pdf

Das, S. K., Kant, K., & Zhang, N. (2012). Handbook on securing cyber-physical critical infrastructure. Elsevier. Retrieved from https://books.google.co.kr/books?hl=en&lr=&id=MftTeQivgA0C&oi=fnd&pg=PP1&dq=Handbook+on+Securing+Cyber-Physical+Critical+Infrastructure&ots=btXJyS5P37&sig=evhxiS3RLF4bZd5OXxvgImspQ_g

Denning, D. E. (2008). The ethics of cyber conflict. In K. E. Himma & H. T. Tavani (Eds.), The handbook of information and computer ethics (pp. 407–428). Wiley. Retrieved from https://books.google.co.kr/books?hl=en&lr=&id=ZC7SDyPZUMoC&oi=fnd&pg=PA407&dq=victims+of+cyber+conflict&ots=lcfZIdxY72&sig=FwXaBLmrMCzxTwpKGasbGhVli0k

Eom, J. H., Kim, N. U., Kim, S. H., & Chung, T. M. (2012). Cyber military strategy for cyberspace superiority in cyber warfare (pp. 295–299). http://doi.org/10.1109/CyberSec.2012.6246114

Erskine, T., & Carr, M. (2016). Beyond "Quasi-Norms": The Challenges and Potential of Engaging with Norms in Cyberspace. In A.-M. Osula & H. Rõigas (Eds.). Tallinn: NATO CCD COE Publications.

European Council. Convention on Cybercrime, Current (2001). Budapest. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Farrell, H. (2015). Promoting Norms for Cyberspace. Cyber Brief. Council on Foreign Relations Press.

Farwell, J. P. (2014). The Media Strategy of ISIS. Survival, 56(6), 49–55. http://doi.org/10.1080/00396338.2014.985436

Gjelten, T. (2013). FIRST STRIKE: US Cyber Warriors Seize the Offensive. World Affairs, 175(5), 33–43. Retrieved from http://www.jstor.org/stable/43554737

Godwin III, J. B., Kulpin, A., Rauscher, K. F., & Yaschenko, V. (2014). Critical Terminology Foundations 2. EastWest Institute and the Information Security Institute at the Moscow State University. Retrieved from https://www.eastwest.ngo/idea/critical-terminology-foundations-2

Goldman, D. (2016, February). Twitter goes to war against ISIS. Retrieved September 16, 2016, from http://money.cnn.com/2016/02/05/technology/twitter-terrorists-isis/index.html

Gordon, K., & Dion, M. (2008). Protection of Critical Infrastructure and the role of investment policies relating to national security. Investment Division, Directorate for Financial and Enterprise Affairs, Organisation for Economic Co-operation and Development,, Paris (Vol. 75116). Paris, France. Retrieved from https://www.oecd.org/daf/inv/investment-policy/40700392.pdf

Hua, X. (2016, May). China, U.S. discuss int'l norms of state behavior in cyberspace. Retrieved September 15, 2016, from http://news.xinhuanet.com/english/2016-05/12/c_135354264.htm

IMPACT- International Multilateral Partnership Against Cyber Threats. (2016). Retrieved September 15, 2016, from http://www.impact-alliance.org/home/index.html

Information Security Doctrine of the Russian Federation. (2000). Russian Federation. Retrieved from http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument

INTERPOL. (2016). Retrieved September 15, 2016, from http://www.interpol.int/

James, J. I. (2013). An Argument for Assumed Extra-territorial Consent During Cybercrime Investigations. VFAC Review, (25), 7–8. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.711.6146&rep=rep1&type=pdf

Kaljurand, M. (2015, December). International Norms in Cyberspace: A Discussion with Minister Marina Kaljurand. Center for Strategic and International Studies 1616 Rhode Island Avenue, NW Washington, DC 20036. Retrieved from https://www.csis.org/events/international-norms-cyberspace-discussion-minister-marina-kaljurand

Karatzogianni, A. (2013). A cyberconflict analysis of the 2011 Arab Spring. In G. Youngs (Ed.), Digital world: Connectivity, creativity and rights (p. 159). Routledge. Retrieved from https://www.routledge.com/Digital-World-Connectivity-Creativity-and-

Rights/Youngs/p/book/9780415839082

Korzak, E. (2015, September). The 2015 GGE Report: What Next for Norms in Cyberspace? Retrieved September 15, 2016, from https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security Privacy, 9(3), 49–51. http://doi.org/10.1109/MSP.2011.67

Lee, B. (2016). The Impact of Cyber Capabilities in the Syrian Civil War. Small Wars Journal.

Levin, A., Goodrick, P., & Ilkina, D. (2014). Securing cyberspace: a comparative review of strategies worldwide. Montreal, Canada: Canadian IT Law Association. Retrieved from http://www.it-can.ca/wp-content/uploads/conf2014/Securing_Cyberspace-Levin.pdf

Norms of Behaviour for Cyberspace. (2014, June). Retrieved September 15, 2016, from https://www.ccdcoe.org/norms-behaviour-cyberspace

O'Connell. (2016, January). Google Joins the Fight Against ISIS. Retrieved from https://hacked.com/google-joins-fight-isis/

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. (2002). Organization for Economic Co-Operation and Development. Retrieved from https://www.oecd.org/sti/ieconomy/15582260.pdf

Osula, A.-M., & Rõigas, H. (2016). International cyber norms: legal, policy & industry perspectives. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf

Principles of UN peacekeeping. (2008). Retrieved September 15, 2016, from http://www.un.org/en/peacekeeping/operations/principles.shtml

Reed, T. (2007). At the Abyss: An Insider's History of the Cold War. Random House Publishing Group. Retrieved from https://books.google.co.kr/books?id=69Vvboox1JcC

Schmitt, M. N. (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press. Retrieved from https://books.google.co.kr/books?hl=en&lr=&id=FujYDXdOMQgC&oi=fnd&pg=PR1&dq=Tallinn+Manual+on+the+International+Law+Applicable+to+Cyber+Warfare&ots=M1uSBsT3Nu&sig=jwHYrfUIWFhlCl3iZd-q09QzAwM

Schmitt, M. N., & Vihul, L. (2014). The Nature of International Law Cyber Norms. Rochester, NY. Retrieved from http://papers.ssrn.com/abstract=2543520

Segal, A. (2011, March). Cyberspace Governance: The Next Step. Council on Foreign Relations Press. Retrieved from http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397

Solce, N. (2008). Battlefield of Cyberspace: The Inevitable New Military Branch-The Cyber Force, The. Alb. LJ Sci. & Tech., 18, 293. Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/albnyst18&section=11

United Nations. (2008). United Nations Peacekeeping Operations Principles and Guidelines. United Nations Department of Peacekeeping Operations. Retrieved from http://www.un.org/en/peacekeeping/documents/capstone_eng.pdf

United Nations. (2015a). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

United Nations. (2015b, January). Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. Retrieved from https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf

United Nations. (2016). Digital Blue Helmets. Retrieved September 15, 2016, from https://unite.un.org/digitalbluehelmets/

United States White House. (2011). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. White House. Retrieved from https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Watts, S. (2015). Cyber Law Development and the United States Law of War Manual. NATO Cooperative Cyber Defence Centre of Excellence, International Cyber Norms Development (Anna-Maria Osula Ed., Forthcoming). Retrieved from http://ssrn.com/abstract=2650784

