Cyber Peacekeeping

Nikolay Akatyev[1(✉)] and Joshua I. James[2]

[1] Seoul Tech Society, Seoul, South Korea
nikolay.akatyev@gmail.com
[2] Digital Forensic Investigation Research Laboratory, Hallym University, Chuncheon, South Korea
joshua@cybercrimetech.com

Abstract. Until now, many works have focused on attempting to define cyber warfare, as well as appropriate response leading to conflict escalation. Instead, this paper proposes a comprehensive definition of Cyber Peacekeeping motivated by prior research on peacekeeping, cyber conflict and warfare, and international relations in cyberspace. Cyber Peacekeeping works 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. This work defines key terms of cyber peacekeeping, as well as its scope and goals in relation to conflict prevention, mitigation, aftermath containment and cleanup. We then propose a potential organizational structure of Cyber Peacekeeping to support its defined roles and functions. Through a case study of a notable past cyber conflict, examples of practical cyber peacekeeping are shown, as well as the roles that peacekeeping could have played in such conflicts.

Keywords: Cyber peacekeeping · Cyber conflicts · Cyber war · Cyberspace safe layer · International relations in cyberspace · Stability and security · Information clearinghouse

1 Introduction

The term ‘peacekeeping’ was coined in the 1950s and has drastically evolved since. Conceptually, Bellamy et al. [1] defines peacekeeping as peace operations conducted by ‘uniformed personnel with or without UN authorization’ in order to help bring peace and stability. Until now, peacekeeping has normally referred to the physical world, using physical means against physical threats.

However, as computer systems have become a critical part of the lives of billions of people and their governments, cyber-conflict becomes more feasible, potentially more devastating, and more likely to play a role in physical world conflicts. As of yet, however, there are no examples of peacekeeping in cyberspace though some prior works have attempted to define certain aspects of what we will call ‘cyber peacekeeping’.

As described by Lynn III [2] “the Pentagon formally recognized cyberspace as a new domain of warfare”. Since cyberspace is being treated as a new front for warfare, both war and peace in the context of cyberspace need to be considered. However, in the past

J.I. James and F. Breitinger (Eds.): ICDF2C 2015, LNICST 157, pp. 126–139, 2015.
DOI: 10.1007/978-3-319-25512-5_10

several years there has been increasing discussion on cyber-warfare and cyber conflict. Melzer [3] discusses in what conditions cyber attacks can amount to "armed attack". Further Schmitt [4] in Tallinn Manual discusses options of retaliation in cyberspace. However attribution and estimation of threat are still major challenges during cyber attacks [5]. Incorrect attribution or overestimation of the force of retaliation is likely to exasperate already complicated conventional and cyber conflicts.

Nations are currently building cyber-offensive capabilities [6] resembling the so-called 'war atmosphere' described by Lynn III [2]. The result is that a cyber security framework centered on one country can more easily lead to conflict escalation because the retaliation can come directly from the victim country, not from an international organization that can attempt to assess and enact appropriate, yet peaceful, response.

Besides the mentioned academic and political discussions, real-world cases of conflict between Israel and Palestine [6] and allegedly state-sponsored attacks on Estonia [7] and Iran [8] give examples of growing insecurity and instability in cyberspace that has physical-world consequences. In these cases, physical and cyber conflicts are related, where increasing conflict in cyberspace leads to increased physical-world tensions, and vice-versa.

Cahill et al. [9] and Kleffner [10] recognized this situation. They discussed the threat of online propaganda and possibilities of escalation of physical conflicts as result of activities in cyberspace. As a solution Cahill et al. proposed the concept of 'cyber warfare peacekeeping' and Kleffner argued for the necessity of 'peace operations in cyberspace'.

However, these works heavily modeled traditional peacekeeping that has been shown to have limits [1, 11]. Cahill [9] and Kleffner [10] suggested ad-hoc solutions for cyberspace stability and security without proposing a consistent framework. Inheriting these limitations for operations in a quickly changing and globally-connected cyberspace would already inhibit any cyberspace peacekeeping initiatives.

Bellamy [1] described in detail how such a complex tool as peacekeeping suffered from ambiguous interpretation without clear definition, without a consistent framework, and without clear description of goals and functions.

Moreover we are unaware of any prior work that has addressed the problem of the aftermath of cyber-conflicts as well as the threats of re-engineered cyber weapons and consequent necessary cleaning up activities.

Instead of focusing on the appropriate escalation of cyber-conflicts or ad-hoc solutions, we propose an approach focused on a framework for cyber conflict prevention, mitigation and post-conflict containment and rehabilitation, termed *Cyber Peacekeeping*.

1.1 Contribution

In this work we propose a more comprehensive definition of Cyber Peacekeeping (CPK) and a framework describing the goals, roles and functions of CPK.

This work contributes to the area of cyber security, cyber investigation and international relations by proposing a novel approach to cyber conflict cessation known as Cyber Peacekeeping. Further, this work contributes two novel concepts: *cyberspace safe layer,* which is a classification model for critical infrastructure, and an *information*

clearinghouse that attempts to provide unbiased, verified information to reduce the risk of conflict escalation.

2 Trends in Cyber Warfare

To provide a background for design and implementation of Cyber Peacekeeping the current section surveys existing organizations and their efforts in cyber security, cyber investigations and cyber conflicts.

2.1 Existing International Cyber Security Entities

ITU IMPACT [12] is an international organization affiliated with the United Nations (UN), particularly with its International Telecommunication Union (ITU). This organization recognizes specifics of cyberspace such as its global nature, difficulty of attribution and low entry barrier. It demonstrates an example of successful collaboration among public and private actors in cyberspace. Unfortunately, IMPACT focuses mostly on criminal activities and protection of commercial assets. Moreover major players like the U.S., China and Russia do not participate in the organization.

At the regional level, the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) [13] is another example of multilateral cooperation. NATO, along with INTERPOL, the UN and international CERTs conduct training, and in some ways assist in the communication between countries during cyber attacks and investigations.

Many countries now have national CERTs as well as developing cyber policing and cyber military capabilities. These organizations, however, so far are mostly concerned with prevention, mitigation and investigation once cyber attacks occur. Currently there is some uncertainty regarding who should be a first responder to an international cyber attack. Since such attacks are normally difficult to attribute to a specific actor, it is initially unknown whether it is criminal case or a national security issue.

A common function of all existing organizations is the proposal of regulations, training and information sharing. However, cyber conflicts have fast developing active phases which need adequate reaction in a timely manner that many of these organizations do not have the capacity or capability or coordination to handle during major conflicts.

2.2 Examples of Past and Ongoing Cyber Conflicts

In 1982, the explosion of a pipeline in Siberia [14] was alleged to be the first cyber incident that also had physically destructive consequences. Allen [6] describes the alleged first major cyber conflict between Israel and Palestine, which compromised civil services and attracted volunteer cyber warriors for both sides from all around the globe.

Cyber attacks on Estonia [7] in 2007 and Korea in 2011 [8] interrupted normal operations of government services and caused a cyber arms race initiating the creation of NATO CCDCOE in Estonia and Cyber Terror Response Center (CTRC) and Cyber Command in Korea.

Stuxnet [8] was alleged to be the first full-scale state-sponsored operation which targeted and destroyed physical objects. Devastating aftermath followed where criminals reused this sophisticated cyber weapon to attack private corporations.

Continuous tension between Taiwan and China periodically lead to cyber attacks [15] which result in a buildup of cyber-offensive capabilities.

Ongoing conflict between opposition and governmental forces in Syria [16] as well as ISIS [17] have cyber-offensive capabilities. Utilizing information warfare, they attract volunteers both in cyber and physical spaces escalating the conflict.

The described cyber capabilities may be used to escalate the political situation in cyber and physical spaces, threaten critical infrastructure and consequently physical safety, leave devastating aftermath, or everything at once. However, existing organizations are not well positioned to respond to the described threats, if conflicts involve more than one country or region. International CERTs, INTERPOL, and others were unable to help defend Estonia or Korea against massive Distributed Denial of Service (DDoS) attacks. And IMPACT and related organizations could not address aftermath of Stuxnet. While humanitarian missions operate in Syria and coalitions fight ISIS in physical space, no organizations adequately address cyber elements of these conflicts.

2.3 Cyberspace Specifics

Cyberspace is overarching and fast-changing, and has a major difficulty in proper attribution [2, 6, 9]. Further, as has been shown, there is a low barrier to cyber weapon reusability.

A fast-changing and agile cyberspace means that traditional approaches are less applicable to cyberspace issues. Cyber Peacekeeping must consider above mentioned properties of cyberspace in its design and implementation.

3 Cyber Peacekeeping

This section describes a framework for Cyber Peacekeeping that includes descriptions of roles, functions and organizational structure. The goal is that the proposed framework provides a solid foundation for practical implementation of CPK, and points for future discussion of the subject.

The proposed framework is motivated by prior works and the current state of cyber warfare, discussed in sections one and two.

3.1 The Need for Cyber Peacekeeping

American adults are estimated to spend an average of approximately 6 h a day using digital devices [18]. A growing number of people, however, are spending more time with digital devices than without. Cyberspace as a new realm of human activities possesses opportunities as well as challenges. There are a number of prior works describing the benefits that digital technologies provide, such as accessible education, health care and freedom of speech. For every benefit described there are also warnings about the future of cyberspace.

Notably, governments are struggling to find a balance between openness and control of the Internet. With the absence of norms and rules to which governments are accustomed, it also becomes possible to start conducting cyber warfare related operations. If detected, victim States may escalate conflicts by retaliating disproportionately or even potentially towards mis-attributed actors. The spread of cyber weapons among volunteer cyber warriors, terrorists and criminals is another source of escalation. Amidst growing criminal and military threats, espionage will undermine the openness of cyberspace and eventually separate governmental and civil networks that would greatly slow development, as described by Kaspersky [19].

Cyber Peacekeeping is needed to protect an increasingly-connected number of people, to help prevent escalation of cyber conflicts - especially those that may lead to real-world conflict escalation - to provide knowledgeable arbitration among States, and to help build and maintain trust and openness in cyberspace.

3.2 Overview of Cyber Peacekeeping

To carry out its mission, we define goals, roles and functions for Cyber Peacekeeping as shown in Fig. 1.

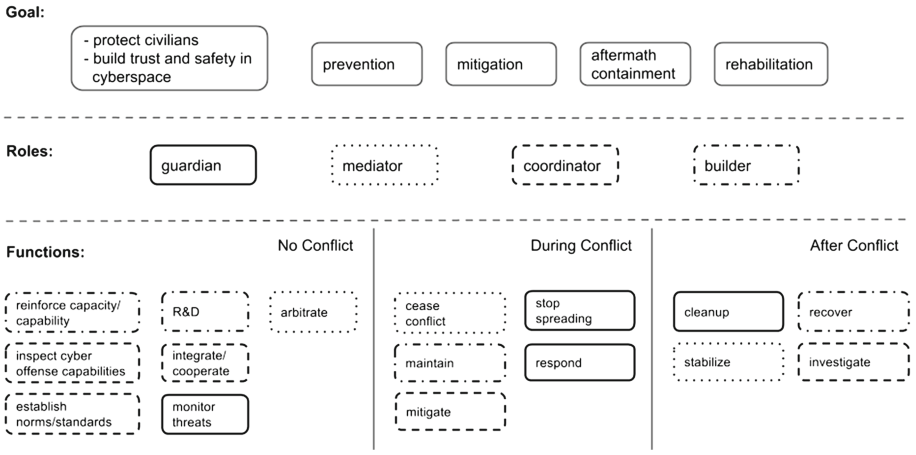

Fig. 1. Overview of the framework of CPK reflecting layers of goals, roles and functions when there is no conflict, during conflict and after conflict. Solid line, guardian role and related functions; dotted line, mediator and related functions; dashed line, coordinator and related functions; dash-dotted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

Each role of Cyber Peacekeeping can contribute to the safety and security of cyberspace at all three different stages of a conflict: no conflict, during conflict and 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 counterattacks as a last measure. After conflict CPK as a guardian will lead cleanup activities related to distribution and alteration of cyber

weapons. In Fig. 1 relations among roles and their functions for different stages of a conflict are depicted by different types of lines: solid, dot, dash, dash-dot.

The goals of Cyber Peacekeeping are defined as:

- Protect civilians
  - The main goal of CPK is the protection of civilians. CPK must be impartial to any State independent of contributions.
- Increase trust and security in cyberspace
  - Through conflict prevention, mitigation and rehabilitation tasks, trust in cyberspace can be maintained and security increased.
- Prevention
  - Focuses on preparation for potential attacks, and preventing cyber conflict escalation when conflicts begin
- Mitigation
  - Focuses on containing conflicts and minimizing damage to infrastructure and civilians
- Aftermath Containment
  - 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
- Rehabilitation
  - Focuses on rebuilding infrastructure, security and trust post-conflict

3.3 Definition of Cyber Peacekeeping

Cyber Peacekeeping is defined as *cyber conflict prevention, mitigation, aftermath containment and rehabilitation with a focus on conflict de-escalation and civilian security*.

Cyber Peacekeeping works to promote online safety and security with accordance to international laws and agreements in order to protect civilians as its main goal. CPK is a framework to maintain conditions for lasting peace in cyber and physical spaces impacted by possible threats in cyberspace. CPK defines specific roles and functions at different stages of peace conditions: no conflict, during conflict, after conflict.

3.4 Roles of Cyber Peacekeeping

As defined, the CPK's main role is the protection of civilians in relation to conflict prevention, mitigation, aftermath containment and rehabilitation. Based on this definition, CPK roles are defined as: *guardian, mediator, coordinator* and *builder*. These roles could be considered similar to departments, each with specific functions at specific stages of cyber conflicts.

3.4.1 Guardian

The guardian engages threats directly using technical, non-offensive means to protect civilians, and maintain peace in cyberspace. The guardian monitors, responds to and

cleans up threats on a technical level. Functions - defined below - are related to helping prevent ongoing attacks, monitoring the decimation of threatening software and cleaning up their aftermath.

3.4.2 Mediator

The mediator engages with threats through activities involving participating actors of a conflict with a goal to reduce threats and de-escalate conflicts. The mediator's role closely models the mediator's role in traditional peacekeeping, where it engages with adversaries to establish and facilitate dialog with the purpose of conflict prevention, cessation and stabilization afterwards. In addition the mediator of cyber conflicts must take into account specifics of cyberspace in order to effectively resolve the conflicts. The mediator relies on norms and standards of relations in cyberspace when attempting to resolve a conflict.

3.4.3 Coordinator

Currently, there are no established norms and standards of international relations in cyberspace. The coordinator will work to develop these standards during peacetime and collaborate with the mediator for their promotion.

Similar to the mediator role, the coordinator functions mostly involve communication. However, while the mediator establishes communication among participating actors of a conflict, the coordinator establishes communication among as many stakeholders of cyberspace as possible including private, public and academic organizations.

Lynn III [2] emphasizes complexity and fast-changing environment of cyberspace, and explains that "U.S. Cyber Command integrates cyber defense operations across the military" for coordinated and fast response to threats. Globally, there are different international stakeholders in cyberspace with different goals and cultures. As a coordinator, the CPK becomes a communication channel for international cyber operations and boosts cooperation across diverse international actors to negotiate control of cyber offense capabilities, establishment of norms and standards. The coordinator supports all other roles facilitating international cooperation to mitigate ongoing conflicts and investigate consequences.

3.4.4 Builder

The builder consistently reinforces the capacity and capabilities of governments, private organizations and critical infrastructure during peacetime. The builder helps to secure computer systems, maintain capacity during conflict and helps recover essential services disrupted or destroyed as the result of the conflict.

3.5 Functions of Cyber Peacekeeping

Each of the above roles have specific functions categorized by the current stage of conflict; No conflict, During conflict, After conflict.

3.5.1 No Conflict

When there is no - detected - conflict in progress, CPK's main role is that of coordinator which must unite efforts to keep safety and stability and to prevent conflicts. The builder role has significant number of functions at this stage as well, including conducting research and development and reinforcing capacities and capabilities of States as well as the CPK itself. The guardian role actively monitors threats, while the mediator attempts to arbitrate any potential conflicts that could escalate.

When there is no conflict, the builder performs long-term functions such as conducting research and development and reinforcing capabilities and capacities of stakeholders in cyberspace. The CPK conducts its own R&D as well as collaborates with academia to develop up-to-date defensive and offensive tools and methods.

Together with law enforcement organizations, the builder provides training to organizations and agencies that are responsible for critical infrastructure and services directly linked to the safety of civilians.

While working with governments, the coordinator analyses trends of international relations in cyberspace in order to guide efforts establishing norms and standards. This task is supported by working with relevant organizations, such as anti-virus companies, to understand the current threat landscape.

To strengthen collaboration among diverse stakeholders the coordinator also helps coordinate cyber defensive drills among participating governments and organizations. ITU IMPACT conducts cyber security exercises aimed to strengthen collaboration among different CIRTs which serve for protection of business [11]. Cyber Commands conduct their military exercises to protect national assets [2] or show the strength of collaboration for deterrence [20]. The main goal of CPK is to protect civilians, so for this purpose the CPK unites and promotes collaboration not only among different cultures and languages but also among different entities such as private companies, national agencies and international organizations.

Further, Allen [6] compared cyber weapons to Weapons of Mass Destruction (WMD). The international community already established treaties and protocols to ensure non-proliferation of WMD. For that purpose the international community applies mechanisms of inspections and sanctions. The CPK can also unite the international community to inspect buildup of cyber offense capabilities including malware, vulnerabilities and surveillance systems.

When detected cyber threats are beginning to escalate conflict, the mediator can engage relevant stakeholders in order to arbitrate conflicting parties and prevent conflict before further escalation.

The guardian is responsible for technically monitoring the current threat landscape, and attempting to identify any stakeholder vulnerabilities and upcoming potential conflicts. Through monitoring of potential threats, the guardian can react to upcoming threats by coordinating relevant stakeholders and offering technical expertise to remove identified threats.

As a synergy of the guardian and builder roles the CPK helps to audit and protect assets identified as key resources, as well as government online services and elements of critical infrastructure. Social engineering methods [21] have been observed during conflicts between China and Taiwan [15]. The CPK audits, educates and promotes secure

use of technology to the public, private organizations and governments. The guardian role is tasked with discovering new technical and social engineering methods.

The guardian independently monitors - but does not block - media outlets to identify content that may result in national or international conflicts. The guardian helps to audit the technical security of key data centers and other online-resources, and collaborates with states to ensure prevention of unauthorized cyber attacks from their infrastructure by third parties.

3.5.2 During Conflict

During a conflict the CPK actively employs its executive and diplomatic functions to stop technical attacks and establish a dialog among conflicting parties. The CPK coordinates actions of the international community to reduce the effects of ongoing attacks, and attempts to rebuild and protect identified critical services - such as health or fire emergency services - in real time.

Impartially to the side of the conflict, as the builder role the CPK must help maintain critical infrastructure and essential services even under severe attack. If a system or service is identified as critical infrastructure, the CPK should have the ability to actively configure systems to ensure their security. In case of web-services, the CPK can add additional computational resources or redirect traffic when such services are under Denial of Service (DoS) attacks.

During conflict, the coordinator must coordinate the actions of the international community to quickly reduce the negative effects of attacks against stakeholders. For example, coordinating ISPs of countries to block IP addresses involved in a DoS attack.

The main task for the CPK in the case of an ongoing cyber conflict is to stop the conflict. As a mediator the CPK can utilize mechanisms of persuasion or coercion to bring adversaries to negotiate [22]. The CPK utilizes support of the international community and stakeholders of cyberspace as a tool for mediation. Clearly established norms and standards of behaviour in cyberspace, which are developed in peacetime, would give the CPK solid ground to negotiate with adversaries.

As a guardian, the CPK actively engages threats to civilians to stop conflicts from spreading and to ensure that any response, if necessary, is legal and proportionate.

Analysis of conflicts in Syria [16] and China [21] shows that participants actively spread hacking tools in order to attract new volunteers worldwide. A key task of the guardian includes monitoring Internet activities [6] which spread malware or explicitly provide hacking tools for volunteers, like in the case of the conflict between China and Taiwan [21]. The guardian identifies and helps to block sources attempting coordinate attacks through the spread of tools or volunteer hacking [6].

During conflicts, the guardian can also provide objective and verified information in response to propaganda spread in media and social networking service. The CPK is not a censor, but instead provides a platform for the distribution of verified information, and clearly indicating what information cannot be substantiated. The CPK will use the same communications channels to attempt to distribute information provided in this verification platform.

3.5.3 After Conflict

After conflict the CPK attempts to stabilize the situation, and prevent further destruction or recurrent attacks. Little attention has been given to the problem of recovery and cleanup from the aftermath of cyber conflicts, though there are real-world examples of how cyber weapons and their descendants [8] are spread and may harm civilians, such as Stuxnet variants like Duqu and Gauss.

After conflict, the builder helps States to recover their critical infrastructure and essential services which were damaged during the conflict. The builder analyzes identified weak points in protection of critical infrastructure and services, and helps to reinforce capabilities and capacities for their protection.

Partnering with public and private actors, the coordinator collects and analyzes cyber weapon samples, and helps produce countermeasures for governments, organizations and civilians. These guidelines are also technically implemented in practice through the builder and guardian roles.

The CPK also facilitates cooperation among diverse stakeholders in cyberspace in order to find - and properly attribute - attackers, prevent further attacks and show examples of accountability. The coordinator helps to investigate cases, attribute attacks and supervise enforcement of local and international law.

Once conflict is finished there is still a high possibility that adversaries would re-engage. The mediator continues efforts to establish dialog among adversaries and to stabilize the situation with the purpose to prevent further conflict. Unlike traditional warfare with spatially localized effects, cyberspace is interconnected and the results of attacks spread globally. This means that each adversary must collaborate to eliminate consequences in cyberspace. The mediator attempts to involve past adversaries in the activities to cleanup the aftermath and control cyber offensive capabilities.

Post-conflict, the guardian's goal is monitoring and prevention of descendants of cyber weapons and viruses. The guardian is responsible for identifying what cyber weapons were used, and how. This information is used to improve threat monitoring, and building protections for systems. Further, by monitoring cyber weapons, guardians can help prepare law enforcement and private organizations for crime-related derivative malware that emerges.

3.6 Implementation of Cyber Peacekeeping

In this section we propose specific, practical functions that CPK could begin that would immediately have real-world impact. The described functions of CPK can be divided into two categories depending on whether the tasks are urgent or long-term. These categories are defined as Rapid Response Division (RRD) and Long-term Stability and Relief Division (LSRD). These divisions and their main functions are shown in Fig. 2, with functions further described in Table 1.

Table 1 categories functions of RRD and LSRD. We described all functions and their impact in the Sect. 3.5. Here we attempt to analyze how these functions can fit to the concept of immediate and long-term tasks.

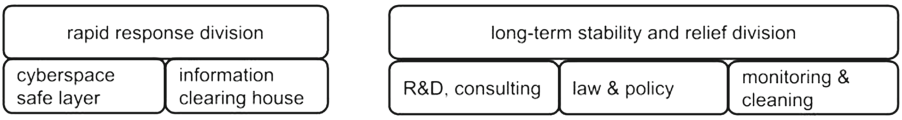

Fig. 2. Overview of the structure of Cyber Peacekeeping implementation divided into Rapid Response and Long-Term Stability Divisions with their corresponding main functions.

Table 1. Rapid Response Division and Long-Term Stability and Relief Division functions lists.

Rapid Response Division functions	Long-Term Stability and Relief Division functions
• monitor threats • arbitrate potential warring parties • cease conflict • stop spreading of threats • respond to aggressors • maintain cyberspace safe layer • maintain information clearinghouse • mitigate the effect of attacks • cleanup consequences • stabilize the situation	• reinforce capacities and capabilities • conduct R&D • inspect cyber offense capabilities • establish norms and standards • unite stakeholders • monitor threats permanently • mitigate the effect of attacks by international cooperative efforts • cleanup all consequences • recover critical infrastructure and services • stabilize for lasting peace and security • investigate and attribute

3.6.1 Rapid Response Division

The RRD is a response to the described overarching specifics of cyberspace and fast-changing situations online. The RRD mostly operates in conditions of ongoing cyber conflicts which may escalate and spread quickly, making immediate response necessary.

The RRD focuses on the protection of the *cyberspace safe layer (CSL),* which is the pre-identified, minimally-required critical infrastructure necessary for civilian safety. Prior research describes the necessity to protect critical infrastructure [23]. However, there is no mutual agreement about definition what constitutes critical infrastructure in different countries. Here, the CPK together with the international community and individual States should attempt to define minimal critical infrastructure required for civilian safety. The CSL then becomes the focus of CPK when conflicts arise in the country or region.

The guardian role of CPK provides protection of CSL when there is an ongoing conflict, meanwhile for the mediator it becomes the first goal of negotiation with warring parties in order to prevent their attacks on the CSL.

The builder must audit and improve security of the assets included in the CSL at the first place, maintain its endurance during the conflict and recover after the conflict.

The main function of the coordinator is to define minimally-required critical infrastructure among most of the stakeholders in the international community.

Another equally important part of conflict de-escalation is the management of an *information clearinghouse (ICH)* 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 guardian will collect, analyze and publish objective information. The builder will research and develop the infrastructure to run the ICH. And the coordinator will engage the international community for the participation in the ICH.

3.6.2 Long-Term Stability and Relief Division

The LSRD acts to ensure long-lasting peace and stability. The LSRD partially inherits its structure from ITU IMPACT and CERTs together with our proposal of a monitoring and cleaning team that responds to the threats of aftermath of cyber conflicts.

The LSRD performs long-term tasks such as tier-based capacity and capability building through R&D and consulting, facilitating dialog in the international community to establish norms and standards in cyberspace, monitoring potential threats in unstable environments and monitoring threats remaining after conflicts to clean them up. Further, the LSRD coordinates training, intelligence and defense capabilities among public and private stakeholders in cyberspace.

4 Case Study

This section attempts to demonstrate how Cyber Peacekeeping may be applied to real cyber conflicts. In this example, the ongoing conflict between Taiwan and China has been chosen.

Taiwan and China have deteriorating diplomatic relations, and are periodically involved in cyber conflicts against each other [15]. These cyber conflicts attract civilian volunteers from both sides, and include attacks on government services and defacing political websites. Recent cases described by [21] involve social networks exploited to get information about military staff for malicious purposes and social engineering.

Such cyber activities reignite tensions in the physical world and stimulate a buildup of offensive cyber capabilities. As a coordinator, in the long-term, the CPK will attract attention of the international community to the problem. The CPK can engage to facilitate mutual understanding and stress the mutual - and collateral - danger when cyber weapons are used.

As a builder the CPK would monitor technical and social engineering methods from both sides in order to educate personnel of critical services, and build cyber security capacity in the cyberspace safe layer for both countries. Further having an attack on the cyberspace safe layer the guardian will protect it.

For cases involving media and social networks, an information clearinghouse as an implementation of a guardian role will provide objective and trustworthy information to attempt to reduce the attraction of volunteers, where possible.

When the cyber conflict has stabilized, as a mediator the CPK will attempt to facilitate a dialog between recently warring countries and help establish mutual agreements

and collaboration to cleanup defaced websites and minimize the spread tools used during cyber attacks. As a guardian the CPK would explicitly participate cleaning up consequences of the conflict. At a global landscape, the coordinator will unite the efforts of the international community to assess consequences of the conflict and investigate its cause and aftermath.

While CPK alone is unlikely to bring peace between countries at war, this case shows that CPK can be employed at different stages of peace conditions and can be a practical tool to help with prevention of escalation of conflicts like those seen in Taiwan vs China [15] or Israel vs Palestine [6], as well as helping with the prevention of a cyber arm race which happened in South Korea [8], Estonia [7] and Taiwan [15].

5 Conclusions

Cyber Peacekeeping is a large, very difficult subject, but one that will need a practical solution as cyberspace is increasingly used for terror, espionage and war. Currently, international relations are not at a point where truly global Cyber Peacekeeping is possible. Implementation at a regional level is also undesirable since many regions already have organizations that have at least some overlap with Cyber Peacekeeping, as proposed. Instead, already established international organizations, such as INTERPOL or the United Nations, should attempt to fill the identified gaps. The challenge then would be allowing Cyber Peacekeeping to remain agile and responsive while being associated with large, notoriously slow entities.

Alternatively, some described aspects of Cyber Peacekeeping could be implemented regionally, such as the concept of a cyberspace safe layer, and information clearinghouse. If these are established regionally, or even nationally, then once a global entity for Cyber Peacekeeping does exist, current local implementations and standards could be directly applied.

5.1 Future Work

Cyber Peacekeeping is still a new, untested idea. Future work will focus on discussions and feedback from potential stakeholders as to the practicality of the roles and functions that have been identified.

Specifically, future work will continue to develop the concept of a cyberspace safe layer, possibly for national use and assessment. Likewise, the practicality of an information clearinghouse will be explored by building prototypes and assessing their performance against past conflict escalation events.

References

1. Bellamy, A.J., Williams, P.D., Griffin, S.: Understanding Peacekeeping. Polity, Cambridge (2010)
2. Lynn III, W.J.: Defending a new domain: the pentagon's cyberstrategy. Foreign Aff. **89**, 97–108 (2010)

3. Melzer, N.: Cyberwarfare and International Law. UNDIR Resources, Helgafell (2011)
4. Schmitt, M.N. (ed.): Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, Cambridge (2013)
5. Hathaway, O.A.: The Law of Cyber-Attack. Faculty Scholarship Series. Paper 3852 (2012)
6. Allen, P.D., Demchak, C.: The Palestinian-Israeli Cyberwar. Mil. Rev. **83**, 52 (2003)
7. Rehman, S.: Estonia's Lessons in Cyberwarfare. USNews (2013)
8. Boo, H.-W., Lee, K.-K.: Cyber war and policy suggestions for South Korean planners. Int. J. Korean Unification Stud. **21**(2), 85–106 (2012)
9. Cahill, T.P., Rozinov, K., Mule, C.: Cyber warfare peacekeeping, pp. 100. In: Proceedings of the 2003 IEEE Workshop on Information Assurance (2003)
10. Kleffner, J.K.: Keeping the cyber peace: international legal aspects of cyber activities in peace operations. Int. Law Stud. **89**, 1 (2013)
11. Bayo, O.A.: The factors behind success and failures of United Nations peacekeeping missions: a case of the Democratic Republic of Congo. J. Altern. Perspect. Soc. Sci. **3**(4), 19 (2012)
12. ITU International Multilateral Partnership Against Cyber Threats. http://www.impact-alliance.org/
13. NATO Cooperative Cyber Defense Center of Excellence. https://ccdcoe.org/
14. Bronk, C.: Hacks on Gas: Energy, Cybersecurity, and U.S. Defense. Rice University, Houston (2014)
15. Chang, Y.: Cyber conflict between Taiwan and China. Strateg. Insights **10**(1), 25–35 (2011)
16. Farwell, J.P., Arakelian, D.: A Better Syria Option: Cyber War. The National Interest (2013)
17. Al-Marashi, I.: The Angel of Death is coming for you, ISIL. AlJazeera (2015)
18. Mobile Continues to Steal Share of US Adults' Daily Time Spent with Media. eMarketer (2014)
19. Eugene Kaspersky Press Club 2013. Canberra, Australia (2013). http://outsidelens.scmagazine.com/video/Eugene-Kaspersky-Press-Club-201
20. Kulikova, A.: Is a cyber arms race between the US and Russia possible? Russia Direct (2015)
21. Cole, J.M.: China's Shifting Cyber Focus on Taiwan. The Diplomat (2013)
22. Sartre, P.: Making UN Peacekeeping More Robust: Protecting the Mission, Persuading the Actors. International Peace Institute, New York (2011)
23. Das, S.K., Kant, K., Zhang, N.: Handbook on Securing Cyber-Physical Critical Infrastructure. Elsevier, Amsterdam (2012)