International Journal of Cyber Warfare and Terrorism
Volume 9 • Issue 1 • January-March 2019

Cyberpeacekeeping:
New Ways to Prevent and Manage Cyberattacks

A. Walter Dorn, Canadian Forces College, Toronto, Canada
Stewart Webb, DefenceReport, Salt Spring Island, Canada

ABSTRACT

Cybersecurity is coming to the forefront of the concerns of nations, organizations and individuals. Government agencies, banking systems and businesses have been crippled by criminal and malicious cyberattacks. There are many examples of cyberattacks in regions of tensions and armed conflict. There are no impartial international means to investigate the claims and counter-claims about cyberattacks. The international community more broadly lacks a way to deal with cyberattacks in a concerted manner. A new approach and capability should be considered for certain circumstances: cyberpeacekeeping. Peacekeeping has proven effective in physical space, and many of the same principles and methods could also be applied in cyberspace, with some adjustments. It could help prevent global attacks, and if an attack were to be successful, it could assist with recovery and conduct impartial investigations to uncover the perpetrators. The possibilities of a cyberpeacekeeping team at the United Nations to make cyberspace more secure are well worth exploring.

KEYWORDS

Cyber Operations, Cyberpeacekeeping, Cyberterrorism, Peacekeeping, Tallinn Manual

1. INTRODUCTION

1.1. The Challenge

The world is ever increasingly reliant on internet-connective technology. Computers permeate almost every facet of human life in most parts of the world, connecting people in ways that could not have been imagined, with the developing world becoming connected at the fastest rate. The level of technology and global integration is staggering even compared to just 20 years ago. This interconnectivity is a cause not only of celebration but also of deep concern for security, as what makes human life easier and more efficient also gives rise to significant vulnerabilities and threats, even the potential for a massive downfall.

Attacks on global interconnectivity have become a reality. Deliberate attacks are conducted by states or state-sponsored entities or groups or non-state and criminal actors who seek to infiltrate and bring down sites and alter the instructions that computers give to industrial machinery, such as centrifuges, dams and even electric power grids (United States Computer Emergency Readiness Team,

DOI: 10.4018/IJCWT.2019010102

2018; Industrial Control Systems Cyber Emergency Response Team, 2016). Already we have seen the internet, including the parts of the deep/dark web, used to incite riots and even to influence the course of national elections. For instance, new evidence is continually emerging of Russian attempts to interfere in numerous elections, including those of the United States and France (Greenburg, 2017; Pope, 2018). Shortly before Russia invaded Georgia in August 2008, it launched a barrage of Distributed Denial of Service (DDOS) attack, making Georgian military movements and operations so much more difficult and dangerous (Markoff, 2008). The United States and Israel likely introduced malware to cause breakdown in Iranian centrifuges at Natanz. These examples show how cyberattacks have translated into kinetic damage. One problem is that, despite the effects, attribution is difficult and international means for impartial investigation are lacking. Examples of attacks are plenty, but effective responses are few and modest.

At present, the world relies on national security services and commercial companies to handle national cybersecurity, and there is no international body to provide some form of international cybersecurity. While a few countries are developing advanced cybersecurity measures, they still remain vulnerable and most countries of the world have limited capacity to respond to cyber threats. Moreover, there has not been a coordinated international effort to address cybersecurity or create measures of common or collective security in global cyberspace. With many cases of international and intranational conflict, cyberattacks have the potential of unsettling an already fragile peace. This paper seeks to explore new means of addressing cybersecurity, building on the characteristics and successes of peacekeeping in physical space. The paper proposes that the establishment and activities of a UN cyberpeacekeeping unit could lessen the threat of conflicts, help recovery, maintain balance and improve cyber relations in a wide range of scenarios. Examples from the past threats can help illustrate the threats and the types of cases where cyberpeacekeeping could help.

2. EXAMPLES AND MULTILATERAL RESPONSES

In 2007, the Estonia case demonstrated how extensively cyberattacks could affect an entire country. The attack was likely in response to the removal of a Soviet-Era statue of the Bronze Soldier of Tallinn. This showed how actions in physical space can have ramifications in cyberspace. The removal of the statue represented the shift away from Estonia's recent Russian history and domination. Russia not only protested but, in all likelihood, supported a massive cyberattack. An impartial determination of responsibility was lacking, and Russia could easily dismiss and ignore the allegations. But it could increase its threatening power from the suspicions while also punishing Estonia severely.

The widespread and large-scale DDOS attack campaign was unleashed. Banks were shut down, government employees were unable to send emails to one another and the media found it difficult to publish stories. Regular life in Estonia turned to confusion, probably with a few final strokes of a keyboard far away. Only after much effort were computer services restored.

In consequence Estonia, which had joined the North Atlantic Treaty Organization (NATO) in 2004, offered to host a new NATO cyber defence centre. The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) was established in 2008 as a multinational and interdisciplinary hub of cyber defence expertise based in Estonia's capital, Tallinn.[1] Although the centre was created to help meet the collective defence needs for its NATO members, the NATO CCD COE developed the world's first, and most in-depth, analysis on the international law applicable to cyberattacks in an armed conflict situation.[2] Despite the important commentary in the *Tallinn Manual on International Law Applicable to Cyberwarfare* (henceforth Tallinn Manual, currently in version 2.0), the legalities of what constitutes a cyberattack and appropriate responses have not been fully flushed out yet. And the NATO COE cannot be considered an impartial investigator or upholder of any international cyber law, especially since it is biased in favour of NATO and Western countries.

A small but more important legal step had been made earlier in Europe. The Council of Europe drew up in 2001 the Budapest Convention on Cybercrime, the first international treaty

regarding cybercrime. The Budapest Convention was the first international attempt of outlining the legal definitions concerning cybercrimes, which included illegal access, interception of data, data interference, computer-related fraud and forgery and other offences. An Additional Protocol to the Convention entered into force in 2003, adding the dissemination of racist and xenophobic material to the list of cybercrimes (Council of Europe, 2003). The glaring criticism with the Budapest Convention is that it has not been continually updated to keep up with evolving threats and technology (Celik, 2017, p. 106). In order for the Convention to be effective, there needs to be an evaluation schedule so new threats and technology can be added.

The *Tallinn Manual* does not have the legal stature of the Budapest Convention but it does deal with a wider range of cyberattacks and cyberwarfare issues. It is an authoritative but not a unanimous legal interpretation when it comes to the definitions and limitations on cyberwarfare. Within five years of the Tallinn Manual 1.0, a second version was published and addressed some concerns raised after the publication of the first Manual (Jensen, 2017, p. 738). Eventually many of the rules explored in the manual will need to be translated into precise legal instruments.

The consequences of cyberattacks can be dire, even crippling for an attacked state. And they are happening against NATO member states. But because of the lack of an immediate physical threat, NATO is wary of triggering the organization's Article 5, which calls for NATO members to come to the collective defence of one or more members when are under attack. So, cyberattacks on NATO countries and more generally have become a more subtle way of causing havoc without much chance of retaliation (Mustonen, 2015). This, of course, is the challenge of maintaining, or building, peace and law enforcement between to states. Impartial investigation and prosecution followed by enforcement is lacking.

Other regional organizations are wrestling with means to secure the cyber domain, and small steps have been taken. In 2004, the Organization of American States (OAS) adopted a resolution titled "The Inter-American Integral Strategy to Combat Threats to Cyber Security," which placed cybersecurity under the realm of the OAS' Inter-American Committee against Terrorism and called for greater regional cooperation (Organization of American States, 2004). The OAS created Computer Security Incident Response Teams (CSIRTs) that handle "alert, watch, and warning" responsibilities in each member state (OAS, 2018). Similarly, for the Shanghai Cooperation Organization, which is comprised of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Uzbekistan, India and Pakistan, aims to improve the political, economic and security relations, including cyber security, amongst its members. In 2009, the SCO came to an "Agreement on Cooperation in the Field of International Information Security" (Shanghai Cooperation Organization, 2008). This Agreement lays the foundations for the SCO to counter destructive cyberattacks on one of its member states. Once again, it is not an impartial international body but a grouping of states, heavily influenced by regional political agendas and seeking some measures for cyber defence.

Though not approaching the problem globally or impartially, the incorporation of cyber defence in such multilateral alliances highlights the seriousness of cyberthreats. In fact, small cyberattacks might even cause wider cyberwars, if the attacks escalate to alliance-level responses. There is also the real possibility that a major cyberattack could incite a conventional military response in the physical world, particularly in cases where cyber-kinetic weapons like Stuxnet (W32.Stuxnet, 2017) are deployed. Means and models for cyber-de-escalation need to be considered. Undoubtedly, some of the lessons and practices from conflict management between nations and between armed parties can apply in cyberspace. One proposal to explore is peace operations in cyberspace or cyberpeacekeeping.

3. KEEPING THE PEACE IN CYBERSPACE

Cyberpeackeepers, possibly working for the United Nations or mandated by it, could patrol and act in cyberspace in a similar fashion as current UN peacekeepers patrol and act in selected conflict zones of the world. Cyberpeacekeepers could investigate major attacks and hacking events in accordance with

their specific mandates — narrow or broad. Like their current physical counterparts, they could be tasked to reduce tensions between specific nations or other conflicting parties, prevent escalation of cyberwars, and help catch global cybercriminals. They could even assist with rebuilding governmental computer systems or critical infrastructure, such as financial and media services, after a damaging attack. Eventually, international action could be taken to help enforce new cyber rules after impartial determinations of the sources or modes of an attack are made. All these means are currently lacking in the weakly protected cyberspace.

The proposal is relatively new (Dorn, 2017)[3] but there was already some movement in this direction at UN headquarters. In 2013, the UN General Assembly examined the increasing security risk of information and communication technologies (ICT) affecting the security environment (United Nations General Assembly, 2013). Also in 2013, the Chief Executives Board for Coordination adopted seven principles to help member states "respond to cybercrime and cybersecurity needs in the Member States" and "focus on assisting the Member States to take evidence-based action" (Chief Executives Board for Coordination, 2014).[4]

The UN's Office of Information and Communications Technology (OICT) created in 2016 a "Digital Blue Helmets" (DBH) unit to "enhance cybersecurity preparedness, resilience and response," mostly for protection of the United Nations and its agencies (United Nations, 2017a). The OICT conducted research into possible cyber threats to the UN's Sustainable Development Goals. It has envisioned DBH centres to provide the necessary "interdisciplinary cyber-security support and teaching centres [to] bring together specialists from around the globe to address a variety of IT-related issues" (United Nations, 2017b). With the DBH name incorporating the term "Blue Helmets" (i.e., an informal name for peacekeepers), it foretells of possibility that the unit could possibly prevent, mitigate and deal with global cyberattacks in the future.

The DBH has not yet assisted governments to investigate cyberattacks or help prevent attacks but it has helped make UN peacekeeping operations more secure and helped certain UN agencies, such as UN Office on Drugs and Crime.

Establishing an international cyber forensics team is necessary for the cyberpeacekeeping concept. It could be based on the DBH team that is now gradually developing more expertise. Many attacks are done through hackers who may or may not have formal affiliations with governments and those hackers often mask or change their IP address, which makes it harder to identify them. As Brenner (2007, p. 420) asserts, determining where cyberattacks originate "can take months or even years when digital evidence is fragile and can disappear by the time the investigators obtain the assistance they need." The DBH team could undertake a role that would help with the investigation of a cyberattack when requested. This could follow the example of other governmental organizations such as the National Cyber Security Centre (NCSG) in the UK, or Europol's EC3. The newly formed Canadian Centre for Cyber Security (CCCS) may also be a potential model where the CCCS collaborates not only with the private sector, but also those in academia (Communications Security Establishment, 2018). These governmental organizations provide support for cybercrime investigations.

As outlined by Robinson, et al (2018, p.3), a future DBH team could be comprised of personnel assigned by Cyber-Contributing Countries (CCCs), Cyber-Contributing Organizations (CCOs), volunteer experts and UN cyber staff. This mix of cyber staff loaned and vetted from various countries, international organizations, the private sector, non-governmental organizations and academia could engage in selected projects according to their expertise and impartiality. Although the pool of potential personnel may appear large, finding well trained, and specialised staff from countries and organizations may be a challenge. However, the United Nations has overcome such problems in the past when assembling peacekeeping operations, fact-finding missions and inspection bodies.

In the future, as cyberpeacekeepers gain experience and help from advanced cyber nations (including experts on loan, as is done in physical peacekeeping), they could help in real-time to stop cyberattacks, mitigate the impact of such attacks and assist in re-establishing normalcy by reversing the effects of the attacks. Cyberpeacekeepers could also monitor their cyber area of responsibility to

the extent possible to promote a lasting cyber peace between two countries (Robinson, et al., 2018, p. 6). The UN cyber rescue crew could help members of the international community in times of urgent need.

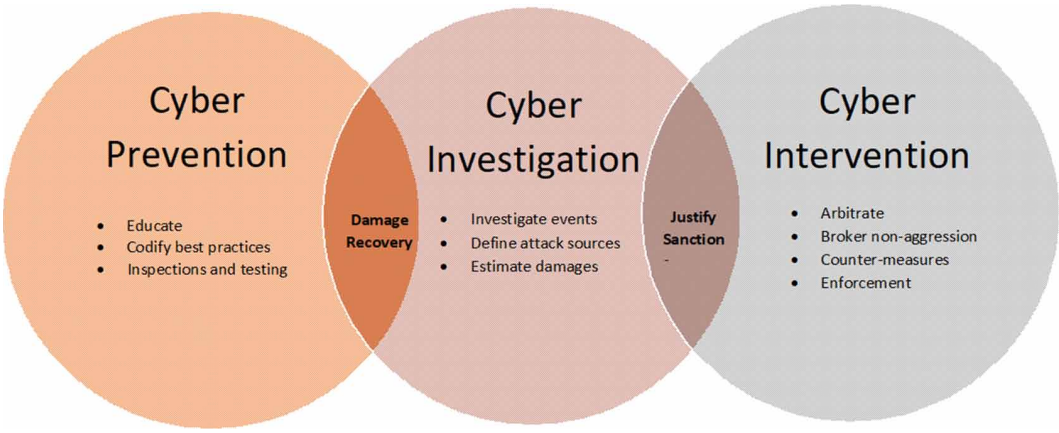
The UN would have to define the parameters of the cyberpeacekeeping force and its cyber areas of responsibility, which could change with demand. It would have to define the how the cyberpeacekeeping unit "could operate in conflict and non-conflict areas in cyberspace" (Akatyev & James, 2017, p. 33). The UN cyberpeacekeeping force could be expanded to investigate mass bot-generated propaganda. In any case, the force would need the cooperation of key UN member states and national organizations.

There could also be a research and development dimension. Exploits and malware seek weaknesses within code and even with human nature — for instance, simple cases of not updating software and website plugins, or even clicking on an attachment in an e-mail without thinking of the risks. One possibility would be to assist in the development of cyber protocols for government, and other sectors. This could start simply with seminars on straightforward measures in ensuring that a potential outbreak can be contained. It will take time for the UN and the international community to create binding global standards and rules, starting though declarations and resolutions and moving on to treaties, to make certain cyberattacks illegal globally.[5] In addition, cyber security measures could be taken between states bilaterally or in small groups, with cyberpeacekeepers playing a role in the implementation.

Of course, one of the limitations of the international order, and an avenue that needs to be developed further, is enforcement. A defensive cyber force would require rules of engagement that may or may not be limited to the digital realm. A defensive action could be to simply block attacks coming from a certain IP address or groups of IP addresses, but it could also mean dealing with the attackers in cyberspace or even the physical seizure of their computer equipment through national law enforcement agencies after determining the attack's point of origin. An overview of the potential range of cyberpeacekeeping tasks is given in Figure 1.

A cyberpeacekeeping operation could be approved by the Security Council, just as the Council approves a peacekeeping operation in the physical domain. In addition, a cyber operation can be approved alongside a physical operation or be a part of it, particularly if the physical conflict includes cyberattacks. If the conflict is entirely in the cyber realm, a purely cyber mission could be instituted. While UN action against major powers is unlikely, due to their veto, there have been important cases where they have called for UN assistance to resolve disputes between them, e.g., the Cuban Missile Crisis of 1962 (Dorn and Pauk, 2009). Moreover, there are cases in conflict regions and even current peacekeeping operations where a cyberpeacekeeping initiative is needed. The prevalence of these

Figure 1. Possible UN cyberpeacekeeping activities



cyberattacks in the present-day world also provides incentive for the affected countries to seek out assistance from a cyberpeacekeeping third party.

4. CYBERATTACKS IN CONFLICT REGIONS

If we look at the attacks of the past, we can see cases where a cyberpeacekeeping capability would have been useful. For instance, North Korea is believed to be behind cyberattacks directed at banks in at least 18 countries, according to the Russian firm Kaspersky (Pagliery, 2017), which itself is suspected of being under the influence, if not control, of an authoritarian state (Robertson & Riley, 2017). So, once again, an impartial means of investigation would be helpful to examine the preliminary data and investigate further. Just as physical peacekeeping uses soldiers borrowed from nations, the cyberpeacekeeper teams could consist of cyber-warriors and experts draw together from nation states for a particular mission or time period.

A UN cyberpeacekeeping force can assist in tracking down the vectors of attack and even point of origin and create the framework for legal or diplomatic action. The threat, and reality of, cyberattacks are a global threat and reality. States should bear a degree of responsibility if an international cyberattack, like any attack, originates from their state (Couzigou, 2018). But great expertise is needed to pinpoint the course of attacks.

Israel was targeted in a cyberattack in 2009 during its offensive in the Gaza Strip. It is believed that it was carried out "by a criminal organization from the former Soviet Union, and paid for by Hamas or Hezbollah" (Pfeffer, 2009). But these are simply allegations, ones that need to be investigated and verified. Particularly, if the allegations are used to launch military attacks, it is important to have some international verification process. Such a verification process needs to be independently run by an impartial body, such as the United Nations, even if it relies of inputs from member nations.

Cyber incidents can also affect countries that host UN peacekeeping missions. For instance, cyberattacks started in the late 1990s between India and Pakistan, which host in Kashmir a UN observer mission (Vatis, 2001), which itself must be protected. The attacks between the nations in the 1990s may be simple and crude compared to what is happening now globally, but Indian and Pakistani hackers have continued to hone their skills. In January 2017, Indian hackers are believed to have attacked Multan International and Karachi airport websites and even installed ransomware, a malware that encrypts a computer's hard drive until a ransom is paid, usually in bitcoins or other digital currency (Shekhar, 2017). This should cause concern, because if an international airport were to be locked out of their computer servers it would cause havoc and increase significantly the chance of casualties. Then both the physical and the cyber peacekeeping force would need to act in a concerted fashion. In addition, a peacekeeping mission could also find itself subject to attack, so a staunch cyber defence will be needed.

One of the main concerns of politicians and security officials is a major cyberattack that cripples the country's power grid, causing many additional catastrophes. A glimpse of this was seen in December 2015, when a cyberattack on Ukrainian utilities resulted in a power outage that affected more than 225,000 customers. The US government later concluded that the power grid shutdown was a cyberattack. iSight partners, now FireEye, concluded that it was carried out by a Russian group, Advanced Persistent Threat, referred to by the cybersecurity community as "Sandworm" (Volz, 2016). A study done by the Electricity Information Sharing and Analysis Center (2016, p. 5) concluded that the perpetrators "perform[ed] long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multisite attack." This attack was planned for some time before it was executed. Regardless, the verification process of which actor carries out these, or future, cyberattacks is essential.

As mentioned, the verification of the attack's point of origin can be a starting point for the local and international authorities to act against such perpetrators—provided it was not sanctioned by a veto-wielding member of the UN Security Council. But even that state's veto of a cyber investigation

could point to its involvement or patronage. And if the cyberattack was sanctioned by another state or a non-state actor, such as a terrorist group, additional actions can be taken to mitigate or punish this activity.

Unfortunately, the global cyber threat is unlikely to diminish, but will increase with time in both the quantity and complexity of attacks, unless some means are found to prevent it. This is especially true for the volatile Middle East and for the ongoing (and deepening) conflict with Iran.

5. STOPPING ESCALATION TO A FULL CYBERWAR

Many became aware of the cyber threats against nations after the attack on Estonia in 2007. The world's attention was refocused in 2010 on targeted attacks by what would otherwise seem to be an inert virus – Stuxnet that targeted Iran's nuclear programme at the Natanz facility. This virus spread itself to several countries, but if an infected computer was not the target, it would do nothing.

Stuxnet targeted Programmable Logic Controllers (PLC) which are usually used for industrial purposes (W32.Stuxnet, 2017). The prevalence of the concentration of the malware in Iran and how the malware targeted PLCs built by the German company Siemens demonstrated that this malware was a surgical weapon to cripple Iran's nuclear program by going after the centrifuges at one of the country's nuclear facilities. Stuxnet can be seen as an improvement or complement to conventional attacks due to the precision and reduction of human casualties. After hundreds of Uranium centrifuges were damaged, suspicions arose that the United States and Israel were behind the Stuxnet attack (Katz, 2010). In any case, forces from within Iran initiated attacks of their own.

In 2012 and 2013, two major attacks seem to have originated from Iran, signalling that the country developed its own cyberwarfare capability in the wake of the Stuxnet attacks. In 2012, over 35,000 computers of Saudi Arabia's Armaco company had their data partially wiped or destroyed (Mount, 2012). Then in a separate attack in 2012, half a dozen American banks were targeted, and their customers were unable to log into their accounts online (Perlroth, 2012). In 2013, hackers were able to gain access to command and control system of a 20-foot flood-control dam on the Blind Brook in Rye Brook, New York (Thompson, 2016). The hacking of this dam would not have caused sizeable damage if the dam waters were to have been released, but it did raise concerns in the United States government about the potential ramifications if a hacker were to seize control of a larger, more critical infrastructure – something similar to what occurred in Ukraine two years later, when a sizeable portion of Ukraine's power grid was shut down because of successful hacking.

Although nations rarely admit to carrying out cyberattacks, the above gives a glimpse of what a full cyberwar could entail. When the sources of attacks can be identified, or at least evidence gathered, by an impartial actor, the chances of an attack and of escalation would be less. And the possibilities for international intervention would be greater. There may be situations where intervention is essential, such as a full-scale cyberattack on a country's cyber-linked infrastructure, e.g., power plants, air and road traffic controls, flood defence controls and the financial sector.

Cyberattacks carried out in the Middle East could possibly escalate to a possible point of no return. The United States and Israel, with Iran in opposition, could have targeted sensitive and critical infrastructure in a series of additional cyberattack exchanges. The mitigating force in this was the restraint demonstrated by the three countries. However, what happens if the states involved in the next exchange of cyberattacks do not demonstrate the same level of restraint? A future exchange could become the cyber equivalent of the Cuban Missile Crisis. In that crisis, the intervention of the United Nations proved crucial to non-violent conflict resolution (Dorn & Pauk, 2009).

Unfortunately, it is not just state actors that can drag two or more states into a cyber conflict; hacker groups can destabilize the international cyber order by carrying out attacks on infrastructure during times of heightened tensions between two states.

This might be mitigated by a cyberpeacekeeping force as it will provide assurances to the international system that there is a check and balance to these attacks and an avenue to pursue, and

help for victims of cyber attacks. It can provide mechanisms that can identify a threat and possibly mitigate, and repair, damage that was done.

6. WHAT WOULD SUCH A FORCE LOOK LIKE?

The UN cyberpeacekeeping force must be malleable and be able to solve a variety of the world's cyber defence issues, not merely one malware or virus at a time. Especially when UN member states further codify a legal set of rules that clearly define what a cyberattack looks like, cyberpeacekeeping could help enforce those rules. For example, the cyberpeacekeepers could help verify that, in times of peace, no state attacks the infrastructure of another and that national enforcement measures are taken by a state if a citizen within the state is found to be the culprit hacker. To further the point: if a Russian hacker is found to be attacking the US government, the Russian government could provide verifiable assurances to the United Nations that the culprit would be arrested and duly processed through the legal system. The United Nations could then verify if this has occurred. This will, at least, put more pressure on governments to hold hackers accountable. Of course, it will need the support of many other governments to apply pressure, as the United Nations seeks to do in many areas, such as human rights, democracy and support of peace processes.

Cyberpeacekeeping can be done in conjunction with regional groups that have cyber defence initiatives. Through the cooperation of these regional initiatives, such as those done by regional organizations, the United Nations can outline what an aggressive cyberattack in peacetime is on a global level. This would assist the international legal framework to define a cyberattack and then help implement international responses.

7. OBSTACLES

The prospect for a UN cyber defence initiative depends on UN member states. They must ask for it. But national cyber defence and offence are closely guarded domains of intelligence and military agencies. By sharing cyber defensive strategies and codes with other members of the international community, the United Nations might make perpetrators more aware of those measures. The same goes for identifying attacks: there will be adaptation. Some member states might not want the United Nations to have the power to launch investigations into cyberattacks and espionage activities as they would be at risk of being uncovered.

One of the fundamental problems is that there are millions of cyberattacks a month and it would be difficult to prevent many of those attacks because of the sheer number. However, the UN cyber defence initiative would only be one actor to serve as a watchful guardian in cyberspace. There could be partnerships with other cyber defenders, though this might face obstacles. For one, a partnership with certain states may not be fruitful since for instance, China, Russia and the United States would be hesitant to share cyber secrets or even alert the UN of cyberattacks that they carry out in most circumstances. However, the UN cyber defence initiative could seek out partnerships with multilateral organizations such as the Shanghai Cooperation Organization or the response teams created by the OAS. When it comes to partnerships with industry, this also may be fraught with concerns over state-influence as we have seen with Kaspersky Labs (Robertson & Riley, 2017). Still, there would be plenty of opportunities to explore partnerships with the wide range of actors and nations, gradually building a network of trusted expertise.

The United Nations has attempted to define what cyber norms should be for the world stage, but those efforts have not been entirely fruitful. For years, the United States hoped that the efforts that it had put in place would be sufficient as a set of norms for the governance of the cyber domain (Grigsby 2017, pp. 111-112). Russia argued that new technology, such as the internet, should require a new treaty, but the United States opposed that position (p. 112). Neither country trusts the other with their cyber intentions. In 2013, the UN Group of Governmental Experts on Developments in the Field of

Information and Telecommunications in the Context of International Security (GGE) put forward a number of cyber norms, for example that in peacetime no country should carry out cyberattacks on another and that such activity should be reported (GGE, 2015, p. 2). It is obvious that a body needs to be created to whom such reports can at least be sent.

The creation of a cyberpeacekeeping unit at the United Nations would mean that countries seeking ways to de-escalate a cyber conflict would have a means to verify an agreement or international standards. The GGE, after several landmark reports, was unable to reach consensus in June 2017 but, in 2018, the High-level Panel on Digital Cooperation was established (United Nations, 2018). This panel also aims to improve digital cooperation amongst countries, private enterprise and other stakeholders. Cyberattacks will undoubtedly be an issue for this panel and cyber peace operations could serve as part of the solution.

More generally, nations have ceded part of their sovereignty to the United Nations when they signed the UN Charter. The Security Council has been given the legal right and responsibility to maintain international peace and security. The Security Council, and to a lesser extent the UN General Assembly, has often responded to world crises with various types of peace operations. The first peacekeeping force, the United Nations Emergency Force, was created to respond to the 1956 Suez Crisis, which it helped resolve. Already for many years previously, the international community and the proposers of UNEF had wrestled with how to apply military force under international control. Similarly, deliberations for a cyberpeacekeeping role can allow the avenues to be explored before the crisis or conflict cries out for a UN role. A cyber peace operation (cyberpeacekeeping) may serve as the tool in a world increasingly defined by cyber interactions.

As we have seen with the creation of regional cybersecurity initiatives in regional organizations, cybersecurity is recognized. But they are regional attempts, not global ones. Having a UN cybersecurity peacekeeping force may seem to be a huge leap, but can easily be a simple step toward ensuring international peace and cyber security.

8. CONCLUSION

There are numerous avenues for the nations of the world to collectively engage in cyber defence. The United Nations, as the world organization responsible for international peace and security, could be pivotal. Even though the concept of digital peacekeeping is new and not fully developed, the United Nations can have a role to motivate member states to look at collective cyber action through the world organization. Cyberattacks are not going away, but they will continue and evolve in sophistication and damage. These attacks have already crippled Estonia in 2007 and a litany of widely ranging attacks have occurred in India, Israel, and Pakistan, to name only a few. Similarly, the United Nations will need to evolve its approach to current and near-future cyberattacks. No longer can peacekeeping operations in the physical space ignore cyber threats against the missions or against the conflicting parties on the ground whom the United Nations seeks to moderate. The safety of the international personnel in foreign lands could be at stake as these cyberattacks become more sophisticated. Similarly, the nations of the world would be wise to explore UN action in cyberspace to protect themselves collectively and thus make the peoples of the world safer.

REFERENCES

Akatyev, N., & James, J. I. (2017). Legislative Requirements for Cyber Peacekeeping. *Journal of Digital Forensics. Security and Law*, *12*(3), 23–38.

Brenner, S. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *The Journal of Criminal Law & Criminology*, *97*(2), 379–475. Retrieved from https://scholarlycommons.law.northwestern.edu/jclc/vol97/iss2/2

Celik, M. 2017. Cyber War: An Expected Apocalypse or a Hyped Threat? In U. Tatar, Y. Gokce & A.V. Gheorghe (Eds.), Strategic Cyber Defense: A Multidisciplinary Perspective (pp. 101-110). Amsterdam, IOS Press.

Chief Executives Board for Coordination for Coordination. (2014, January 13). Summary of Conclusions, Second Regular Session of 2013. UN Doc. CEB/2013/2. Retrieved from https://www.unsceb.org/CEBPublicFiles/Chief%20Executives%20Board%20for%20Coordination/Document/REP_CEB_201311_CEB2013-2.pdf

Communications Security Establishment. Canadian Centre for Cyber Security. (2018). *Government of Canada*. Retrieved from https://www.cse-cst.gc.ca/en/backgrounder-fiche-information

Council of Europe. (2003, January 28). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of the acts of racist and xenophobic nature committed through computer systems. European Treaty Series.

Council of Europe. (2017). Details of Treaty No. 185 – Convention on Cybercrime. Retrieved from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Couzigou, I. (2018). Securing cyber space: The obligation of States to prevent harmful international cyber operations. *International Review of Law Computers & Technology*, *32*(1), 37–57. doi:10.1080/13600869.2018.1417763

Cybersecurity. (2018). Retrieved from https://www.sites.oas.org/cyber/en/pages/default.aspx

Dorn, A. W. (2017). Cyberpeacekeeping: A New Role for the United Nations? *Georgetown Journal of International Affairs*, *18*(3), 138–146. doi:10.1353/gia.2017.0046

Dorn, A. W., & Pauk, R. (2009). Unsung Mediator: U Thant and the Cuban Missile Crisis. *Diplomatic History*, *33*(2), 261–292. doi:10.1111/j.1467-7709.2008.00762.x

Electricity Information Sharing and Analysis Center. (2016, March 18). Analysis of the Cyber Attack on the Ukrainian Power Grid. Retrieved from https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

Greenburg, A. (2017, May 9). The NSA Confirms It: Russia Hacked French Election "Infrastructure." *Wired.* Retrieved from https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

Grigsby, A. (2017). The End of Cyber Norms. *Survival*, *59*(6), 109–122. doi:10.1080/00396338.2017.1399730

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015, July 22). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174 Retrieved from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

Industrial Control Systems Cyber Emergency Response Team. (2016). Year in Review FY 2016 Pie Chart. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf

Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law,* 48(3), 735-778. Retrieved from https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

Katz, Y. (2010, December 24). Stuxnet may have destroyed 1,000 centrifuges at Natanz. *Jerusalem Post*. Retrieved from https://www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz

Markoff, J. (2008, August 12). Before the Gunfire, Cyberattacks. New York Times. Retrieved from http://www.nytimes.com/2008/08/13/technology/13cyber.html

Mount, M. (2012, October 16). U.S. officials believe Iran behind recent cyber attacks. *CNN.* Retrieved from http://edition.cnn.com/2012/10/15/world/iran-cyber/?iid=EL

Mustonen, T. (2015, January 6). DefRep Analysis: NATO's cyber shift may not link to Article 5. *DefenceReport*. Retrieved from http://defencereport.com/defrep-analysis-natos-cyber-shift-may-not-link-to-article-5/

NATO COE CCD. 2017. Tallinn Manual Process. Retrieved from https://ccdcoe.org/tallinn-manual.html

Organization of American States. (2004, June 8). Adoption of a Comprehensive Inter-American Strategy to Combat the Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity. Retrieved from http://www.oas.org/xxxivga/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

Pagliery, J. (2017, April 4). North Korea-linked hackers are attacking banks worldwide. *CNN.* Retrieved from http://www.cnn.com/2017/04/03/world/north-korea-hackers-banks/index.html

Perlroth, N. (2012, September 30). Attacks on 6 Banks Frustrate Customers. *New York Times*. Retrieved from http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html

Pfeffer, A. (2009, June 15). Israel Suffered Massive Cyber Attack During Gaza Offensive. *Haaretz.* Retrieved from http://www.haaretz.com/israel-suffered-massive-cyber-attack-during-gaza-offensive-1.278094

Pope, A. E. (2018). Cyber-securing our elections. *Journal of Cyber Policy*, *3*(1), 24–38. doi:10.1080/23738871.2018.1473887

Robertson, J., & Riley, M. (2017, July 11). Kaspersky Lab has been working with Russian Intelligence. *Bloomberg.* Retrieved from https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. 2018. Developing Cyber Peacekeeping: Observation, Monitoring and Reporting. arXiv:1806.02608

Shanghai Cooperation Organization. 2018. Agreement between the Government of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security (Unofficial English Translation). Retrieved from http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf

Shekhar, S. (2017, January 2). The India-Pakistan cyber war intensifies as retaliatory ransomware attack cripples websites of Islamabad, Multan and Karachi airports. *Daily Mail.* Retrieved from https://www.dailymail.co.uk/indiahome/indianews/article-4082644/The-India-Pakistan-cyber-war-intensifies-retaliatory-ransomware-attack-cripples-websites-Islamabad-Multan-Karachi-airports.html

Thompson, M. (2016, March 24). Iranian Cyber Attack on New York Dam Shows Future of War. *Time Magazine.* Retrieved from http://time.com/4270728/iran-cyber-attack-dam-fbi/

United Nations. (2017a). Cyber Risk. Retrieved from https://unite.un.org/digitalbluehelmets/cyberrisk

United Nations. (2017b). Digital Blue Helmets: Research. Retrieved from https://unite.un.org/digitalbluehelmets/research

United Nations. (2018). Secretary-General's High-level Panel on Digital Cooperation. Retrieved from http://www.un.org/en/digital-cooperation-panel/

United Nations General Assembly. (2013, June 24). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 68th Session. Retrieved from https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf

United States Computer Emergency Readiness Team. (2018, March 16). Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Department of Homeland Security. Retrieved from https://www.us-cert.gov/ncas/alerts/TA18-074A

Vatis, M. A. (2001). Cyber Attacks During the War on Terrorism: A Predictive Analysis. Hanover, New Hampshire: *Institute for Security Technology Studies at Dartmouth College.* Retrieved from www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA395300&Locat

Volz, D. (2016, February 25). U.S. government concludes cyber attack caused Ukraine power outage. *Reuters*. Retrieved from https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K

W32. Stuxnet. (2017, September 26), *Symantec.* Retrieved from https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

ENDNOTES

1 Estonia was a willing host after it suffered a massive cyberattack in 2007 on its websites and cyber infrastructure. The NATO COE was set up to "provide a capability to assist allied nations, upon request, to counter a cyber attack" (NATO summit communique, Bucharest, April 2008). The COE role is to: improve cyber defence interoperability; develop policies, concepts, doctrine, and standards; enhance information security and cyber defence education; provide cyber defence support for experimentation. It also provides cyber defence subject matter experts (SMEs) to NATO, especially for cyber defence testing and validating.

2 The COE led and facilitated the drafting of the influential *Tallinn Manual on the International Law Applicable to Cyber Operations* (version 2.0, Cambridge University Press, 2017). For more information, see: NATO COE CCD. "Tallinn Manual Process." Accessed February 8, 2017. https://ccdcoe.org/tallinn-manual.html

3 See: Nikolay Akatyev and Joshua I. James, "Cyber Peacekeeping," in *Digital Forensics and Cyber Crime*, ed. Joshua L. James and Frank Breitinger (Cham: Springer, 2015), 126-39. Michael Robinson, Helge Janicke, and Kevin Jones, "An Introduction to Cyber Peacekeeping," *Computers and Society*, October 2017. Accessed at https://arxiv.org/pdf/1710.09616v1.pdf. Dorn, A. W. 2017. Cyberpeacekeeping: A New Role for the United Nations?. *Georgetown Journal of International Affairs*, 18(3), 138-146. doi: 10.1353/gia.2017.0046

4 The seven principles can be paraphrased as follows: (1) Cyberincidents should be dealt with in a holistic manner through criminal justice and international cooperation; (2) UN entities should aim to respond to cybercrime and cybersecurity needs in Member States within their respective mandates. (3). All UN programming should respect the principles of the rule of law and human rights; (4) UN programming should focus on assisting Member States to take evidence-based action; (5) Programming should foster a "whole-of-government" response. (6). Support to Member States should aim to strengthen international cooperation; (7) Programming should include efforts to strengthen cooperation between government institutions and private-sector enterprises.

5 The 2001 Budapest Convention on Cybercrime is the first international treaty on crimes committed via the Internet and other computer networks. It deals with things like "infringements of copyright, computer-related fraud, child pornography and violations of network security." It has some early indications of enforcement power through and search procedures of computer networks and interception. See: Council of Europe. "Details of Treaty No. 185 – Convention on Cybercrime." accessed June 12, 2017 http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.