Humanitarian Cyber Operations

Rapid Response to Crimes against Humanity Utilizing Offensive Cyber Ability

Jan Kallberg

Military cyber capacity, built to be a part of military operations, can be utilized for humanitarian operations utilizing the legal framework of responsibility to protect. The responsibility to protect doctrine will allow concerned states to interfere in the domestic affairs of foreign nations that jeopardize the welfare of its citizenry, and the humanitarian operations are not considered acts of war. In principle, cyber can be utilized to protect humanity in the same way as military transportation ships can transport aid to a humanitarian catastrophe.

The growing digital footprint in repressive regimes creates an opportunity for early prevention and interception against the perpetration of atrocities by utilizing the United Nations codified principle of "responsibility to protect" as a justification for the world community, or states that decide to act, to launch humanitarian cyber operations. The principle of "responsibility to protect" would allow foreign interference in domestic affairs without triggering an act of war. Historically atrocities have been identified by the world community up to years after these crimes against humanity were perpetrated. Acquired offensive cyber operations ability can be utilized as a rapid response to the repressive

Digital Object Identifier 10.1109/MTS.2016.2599209
Date of publication: 7 September 2016

regime's planning and staging of crimes against humanity. A primary purpose is to gather information for international intervention, but also to serve as evidence gathering and individual deterrents for those who are in a position to be a part of the execution of planned atrocities. Humanitarian cyber operations enables a faster response, allows retrieval of information necessary for the world community's decision making to occur, and removes the secrecy surrounding the perpetrated acts of totalitarian and repressive regimes.

If a state fails to protect the welfare of its citizens, then states that commit atrocities against their own populations are no longer protected from foreign intervention. Traditionally interventions have utilized military units to intercept the preparation and execution of crimes against humanity. Since the end of the Thirty Year War, and the peace of Westphalia 1648, where states were given the protection of foreign intervention in domestic matters, until recent decades states were guaranteed from other states that there would be no intervention in domestic matters. After the Second World War, and the Nuremberg trials of Nazi war criminals, there was a gradual codification and consolidation of treaties and international and national laws related to crimes against humanity. These have created a well-establish presence and legal foundation for what constitutes crimes against humanity and grounds for prosecution. After the failure to protect the population in former Yugoslavia from atrocities, and the delay in reacting to the genocide in Rwanda, there was a reaction and a responsibility to respond concept developed within the United Nations and the international community.

According to United Nations [1], responsibility to protect can be summarized as:

> Sovereignty no longer exclusively protects States from foreign interference; it is a charge of responsibility that holds States accountable for the welfare of their people.

Responsibility to protect not only enables foreign states to intervene in the domestic affairs of a repressive regime, it is a moral and humanitarian obligation to act. The initial goal is to prevent atrocities, then intercept and hinder further crimes, and if that fails apprehend the perpetrators to be brought to justice supported by international humanitarian law.

Crimes Against Humanity on Trial

The main weakness in the prosecution of crimes against humanity is finding evidence that meets the standards of criminal litigation, where the threshold being that evidence supporting the prosecutor's claim of the defendant's criminal actions is valid and erases any reasonable doubt that the perpetrator perpetrated these crimes. Those who perpetrated crimes against humanity are given a competent defense team, who will examine any evidence and scrutinize its relevance and validity. This will then require a dedicated effort to prosecute, collect evidence, secure evidence, and ensure a fair trial. The International Criminal Tribunal for the former Yugoslavia was organized by the United Nations in 1993 with the jurisdiction determined as:

> …an international tribunal shall be established for the prosecution of persons responsible for serious violations of international humanitarian law committed in the territory of the former Yugoslavia since 1991.

The international tribunal that existed from 1993 expected to have complete all litigation by 2015. During these years charges have been brought against 161 defendants. The tribunal employs 900 staff members. The 900 employees include only the actual staff at the court in the Netherlands; the numerous United Nations, NATO, and national staff in the Balkan region who support the work of the court are not included. The size of tribunal shows the level of resources needed to bring 161 defendants to justice. Digital evidence secured by humanitarian cyber operations could support future litigation and minimize the time consuming and labor intensive traditional evidence gathering.

Noteworthy is that even once the court was created, it still did not serve as a deterrent against atrocities. The massacre after the fall of the town Srebrenica occurred after the tribunal was created. If there is no linkage between the event, the actions, and the defendant that can be evidenced beyond any reasonable doubt, then upholding international humanitarian law fails. And it should rightly fail, because otherwise our war crime judges would sentence defendants based on assumptions and hearsay, making the court proceedings arbitrary and denying the defendant a fair trial.

The pivotal question in upholding international humanitarian law is, how is high quality evidence secured?

Limited Evidence

In a civil war, revolutionary change of government, or societal chaos that is the surrounding environment to these atrocities, documents are lost. A major reason for the success of the Nuremberg Trial of the leaders of Nazi Germany was that Nazi Germany had maintained numerous records and paper trails of the perpetrated events [2]. The Holocaust was well documented in the records retrieved by the Allied Forces after the collapse of the Third Reich. Other perpetrated events, such as the Iranian suppression of opposition and retaliation against former loyalists that occurred from the Iranian Revolution 1979 and forward, lack accessible documentation and tend to not be addressed in the international community because hearsay, witnesses in the perimeter, and accounts of massacres with no link to specific perpetrators do not reach the threshold where prosecution can occur.

Modern civil wars and crises are followed by a flow of migrants and asylum seekers that leave their country of origin and settle in other parts of the world. The migration streams disperse potential witnesses over several continents, creating a challenge to future litigation. The ongoing Syrian civil war has resulted in refugees seeking to reestablish themselves in any country that will allow them to settle. Witnesses can flee the repressive country, be victims themselves, or being silenced by being unable to leave the repressive regime. In cases where crimes against humanity have been successfully prosecuted, the crimes have in most cases been committed in countries where later the law enforcer, or an alliance thereof, occupy the country of the perpetrator. This was the case in Nazi Germany, Iraq, and parts of the former Yugoslavia. If the law enforcers occupy the country where evidence gathering and the process of interviewing witnesses takes place, the process benefits from law enforcers being in control of the territory where the atrocities occurred. In some cases, law enforcement and the pursuit of evidence to support litigation occurred years after the actual events. If laws are upheld years after the actual event they can lose their ability to deter perpetrators to commit further crimes. The law enforcing body is not present at the time of the crime.

International humanitarian law is dependent on evidence gathering, and laws might not be upheld if evidence gathering fails, even if the international community promotes decisive legal action. Humanitarian cyber operations can support the prosecution of crimes against humanity and help generate quality evidence.

Perpetrator's Modus Operandi

Historically, few perpetrators have been brought to justice even if their actions were publically known [3]. It is likely that perpetrators of atrocities expect to avoid prosecution and not be held accountable for these crimes against humanity. The benefits in the moment for being a loyalist to a totalitarian state outweigh the risks involved in engaging in carrying out crimes against humanity on behalf of the totalitarian state.

Therefore, crimes against humanity have been seldom prosecuted compared to other crimes. There are several reasons. The victims, if still alive, and witnesses that survive are silenced by continuing to live in the totalitarian state. During the Stalin era in the Soviet Union, millions witnessed deportation of others or lost relatives and friends in executions of perceived opposition. Millions were prisoners in labor camps or fell victim to other forms of punishment. The Soviet purge of anyone who the ruling regime perceived, arbitrarily, as potential opposition, rendered them either to be executed or sent to harsh labor camps where few survived. The Soviet genocide reached its highest level in sheer numbers subject to repression or execution in the 1920s and 1930s. The Soviet system of repression continued, even if it was less murderous, until the collapse of the Soviet Union in 1990. The only perpetrators of the Stalinist purge in the 1920s and 1930s held accountable for the genocide resulted from the shift of government in the aftermath of the death of Joseph Stalin. These perpetrators were only held accountable for their acts as a way for the totalitarian regime to change its henchmen, not to hold them accountable for their crimes against humanity per se. Secrecy and blocked access to the actual deeds have allowed perpetrators to avoid accountability.

Growing Digital Footprint

Even in states that are authoritarian and totalitarian the degree of network communication, wireless communications, and digital information is growing rapidly, leaving an increasingly large digital footprint. If the states limit access to the global Internet, and other open networks, the digital footprint is still significant. The Democratic People's Republic of Korea, commonly named North Korea or DPRK, utilize a national Intranet as a form of Internet named "Kwangmyong" [4]. These systems are connected to the outer world – no matter if it is not accessible for the average North Korean, it is still accessible for offensive cyber operations.

North Korean cell phone ownership has grown from 60 000 in 2009 to 2.8 million in 2014 [5], and continues to grow. This provides an ever expanding wireless sphere of extractable information. The introduction of cell phones in these repressive regimes is likely driving change [6], and with changing behavior comes an increasing openness about what is shared on the networks.

It is not only the number of cell phones that matters, increased utilization of wireless communications in DPRK creates a larger target area. The pattern is similar in other repressive regimes. The Islamic Republic of Iran had in year 2000 no cell phones, but in year 2002 it had reached 20 000 cellphones, and the latest figure (2014) from ITU estimates 33 000 000 cell phones [5]. An increasing number of cell phones changes behavior. Government officials will share and discuss orders, plans, ideas, allocations, and plans in plain speech either as phone conversations, emails, shared documents, or text messages. The abundance of digital information is a new phenomenon in totalitarian states.

Limitations of Traditional Responsibility to Protect

The high threshold for taking international or unilateral action to according to the obligations to act according to principles of responsibility to protect, is that the action traditionally assumes conventional military intervention. The compliance enforcement of humanitarian law, driven by the intellectual lineage and precedence started in the UN charter of 1945, is intervention utilizing military assets. A repressive nation such as DPRK can, by having a bellicose posture, threaten significant escalation to prevent interference in domestic affairs, and by doing so avoid interference, even if the DPRK regime behind the scenes conducts crimes against humanity (7). If launched, international military humanitarian operations would then automatically turn into to a full-scale conventional war on the Korean peninsula. The DPRK's aggressive stance allows that repressive state to continue human rights abuses without any intervention.

Over the past decade, as the concept of responsibility to protect has developed in the U.N. among international organizations and non-governmental organizations, a concept of a "moral obligation to act" has surfaced (8). The international community, and major powers, cannot silently watch crimes against humanity be perpetrated. There is a moral obligation to act. This is feasible in nations with little military resistance to a humanitarian intervention, such as Rwanda and Sierra Leone. DPRK can mobilize millions of troops. The majority use obsolete equipment, but they are likely to fight hard as a result of decades of propaganda and indoctrination.

A relevant question is, then, whether DPRK can nullify responsibility to protect by their confrontational posture. If that is the case, the worst perpetrator wins. This was already witnessed in the Soviet Stalin terror during the 1920 and 1930s, where accessible documentation afterwards is almost non-existent, the witnesses were to a high degree themselves victims and executed later, and knowledge of these crimes disappeared over time. Historians can estimate the number of killed by the Soviet terror with a granularity of million victims (9), but very few actual perpetrators can be identified and linked to their actual actions.

Launching Humanitarian Cyber Operations

Humanitarian cyber operations can play a role in enforcing international humanitarian law and create access to the secret domains of repressive regimes.

Humanitarian cyber operations are launched under obligations within responsibility to protect, aligned with the United Nations' framework for intercepting and acting to prevent crimes against humanity. The state that utilizes humanitarian cyber operations towards another state declares openly that the state is initiating humanitarian cyber operations in the country of concern.

The open initiation of the humanitarian cyber operations is aligned with responsibility to protect. This avoids having the upcoming events being seen as acts of war, and avoids triggering a just and supported-by-international-law declaration of war by the targeted state.

Humanitarian cyber operations will then be allowed by international law to penetrate the information systems and communication channels of the targeted nation in the pursuit of information that will either confirm or deny that crimes against humanity are occurring within the targeted state. The length and size of the cyber operations is dependent on the initial concern. If a regime systematically, and in defiance of human rights, abuses its population, then the established humanitarian cyber operations continue operating as long as there is a verified concern.

If a country, known for its systematic human rights violations, find itself having humanitarian cyber operations launched against its regime by several major democracies in the international community, the targeted country can appeal in the United Nations. Humanitarian cyber operations are not a carte blanche to conduct offensive cyber operations. Rather they follow the mechanisms of conventional military intervention in failing countries and systematic human rights violation.

There are several benefits of humanitarian cyber operations:

1) Rapid deployment compared to traditional intervention. Cyber operations can be launched within weeks compared to months, generating an ability to quickly gather information.
2) The legal framework is already established in responsibility to protect, Humanitarian cyber operations is another vehicle to reach the intended results.
3) Humanitarian cyber operations limit the advantage that bellicose repressive states receive by having aggressive postures, because these states can not control their digital footprint.
4) Humanitarian cyber operation can be exclusively utilized by functional democracies that respect human rights to protect human life and welfare in repressive states, the repressive states cannot counterstrike at the same level because that might be an act of war, with embedded repercussions.
5) There is no kinetic effect or additional violence, such as a bombing campaign, to soften a repressive regime

to consider policy change, which limits any additional human suffering.

The information gathered by humanitarian cyber operations will come from a variety of sources, depending on need to acquire, based on other intelligence already gathered and on which systems are vulnerable and in reach to penetrate.

In humanitarian cyber operations, communication between dignitaries and administrators who arrange for crimes against humanity can be copied, including orders delivered, and the reports back can be copied as well, which would verify intent, actions, and gather evidence. Information systems that are crucial for the execution of these atrocities can be destroy or severely degraded, such as system systems that support logistics and transportation. Even in a degraded environment, the system failures will create delay and confusion. The perpetrating nations databases used for separating individuals after political belief, ethnicity, religious belief, or any other separator that can be used in an atrocity can be destroyed. If the atrocities are not organized, but the regime organizes information and prepares, then evidence gathering is a primary task for building a case to draw the international community's attention, and to lay a foundation for a case presented to the United Nation and other international forums.

Humanitarian Cyber Operations Provide New Policy Options

By following well-established principles of international humanitarian law's responsibility to protect, repressive regimes can lose protection against foreign intervention, with other state's utilizing offensive cyber operations if there are valid concerns about respect for human rights. Humanitarian cyber operations offer several policy options that were not previously available, allowing policy makers to utilize a less confrontational intervention in another state's domestic affairs. Humanitarian cyber operations will then also increase the quality and granularity in the information at hand for decision making. If an escalation to full-scale military intervention is needed, they can provide information about where human relief is needed.

Cyber operations can also provide evidence to support apprehension of the perpetrators. Due to the fact that humanitarian cyber operations are publically announced, the targeted nation and its nomenclature are made aware that operations are ongoing, which could have a deterring effect at the individual level. The lower echelon potential perpetrators will have to trust that the networks of the repressive regime are not compromised; otherwise they will not fully obey criminal orders because of the risk for future repercussions. Even if 20% of the lower echelon henchmen are diehard in their beliefs and do not care about the consequences, 80% will still covertly respond less eagerly to authority, with a direct impact on the actual execution of atrocities. If a technologically superior nation conducts humanitarian cyber operations against a less technologically advanced authoritarian regime, it is likely that systems are compromised with information leak out of the networks of the perpetrating nation. The complexity of information networks, and the general assumption that major democratic powers are able to conduct deep offensive cyber operations, are likely to create and seed doubt in the minds of individuals who are supporting the atrocities and who are assessing the consequences of participating in crimes against humanity.

Acknowledgment

The views expressed herein are those of the author and do not reflect the official policy or position of the Army Cyber Institute, the United States Military Academy, the Department of the Army, or the Department of Defense.

Author Information

Jan Kallberg is with the Army Cyber Institute at West Point, United States Military Academy, Spellman Hall 4–33, 2101 New South Post Road, West Point, NY 10996. Email: jan.kallberg@usma.edu.

References

[1] United Nations, "The responsibility to protect," Office of the Special Adviser of the Prevention of Genocide, 2016; http://www.un.org/en/preventgenocide/adviser/responsibility.shtml.

[2] A. Tusa, *The Nuremberg Trials*. Rowman & Littlefield, 2003.

[3] J. N. Horne and A. Kramer, *German Atrocities, 1914: A History of Denial.* New Haven, CT: Yale Univ. Press, 2001.

[4] B. Warf, "The Hermit Kingdom in cyberspace: Unveiling the North Korean Internet," *Information, Communication & Society*, vol. 18.1, pp. 109-120, 2015.

[5] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2014; http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/Mobile_cellular_2000-2014.xls.

[6] C. Mims, "Cellphones can spark change in North Korea," *Wall Street J.*, Dec. 7, 2014; http://www.wsj.com/articles/cellphones-can-spark-change-in-north-korea-1417999101.

[7] A.J. Bellamy, "A chronic protection problem: The DPRK and the responsibility to protect," *Int. Affairs*, vol. 91, no. 2, pp. 225-244, 2015.

[8] L. Glanville,"The responsibility to protect beyond borders," *Human Rights Law Rev.* vol. 12, no. 1, pp. 1-32, 2012.

[9] A. Nove, "How many victims in the 1930s?," *Europe-Asia Studies*, vol. 42, no. 2, pp. 369-373, 1990.