United States Military Academy

From the SelectedWorks of Jan Kallberg

Summer July 1, 2015

Bringing Fear to the Perpetrators – Humanitarian Cyber Operations as Evidence Gathering and Deterrence

Jan Kallberg, University of Texas at Dallas

Available at: https://works.bepress.com/jan_kallberg/31/
Bringing Fear to the Perpetrators – Humanitarian Cyber Operations as Evidence Gathering and Deterrence

Jan Kallberg¹

¹Cyber Security Research and Educational Institute, Erik Jonsson School of Engineering and Computer Science, the University of Texas at Dallas, Richardson, Texas, United States

Author biography:
Jan Kallberg, PhD; LL.M., is a researcher at Cyber Operations Lab, Cyber Security Research and Educational Institute, the University of Texas at Dallas and part-time faculty at George Washington University. His works have been published in Joint Forces Quarterly (JFQ), Strategic Studies Quarterly (SSQ), Military Review, Institute of Electrical and Electronics Engineers (IEEE) Access, IEEE Professional, and IEEE Security & Privacy. His personal website is www.cyberdefense.com – a domain name registered in 1996.
Introduction

Humanitarian cyber operations would allow democratic states to utilise cyber operations as a humanitarian intervention to capture information and create a foundation for decision making for collective international action supported by humanitarian international law. This follows the legal doctrine of responsibility to protect, which relies first on the nation state itself but when the state fails to protect its citizens, then the international community can act ignoring the repressive or failed states national sovereignty.

Another support for humanitarian cyber operations is the ability to capture evidence to support future prosecution for crimes against humanity. The weakest link in the chain to prosecute war criminals, and hold those who perpetrate atrocities against civilians are accountable, is secured unquestionable evidence.\(^1\) The quest to secure evidence in the fog of war and turmoil of modern conflicts is a challenging task. In the chaos of civil wars and ethnic conflicts, evidence are lost and witnesses are either casualties of the conflict or dispersed as refugees to other countries, meanwhile the prosecutors need to reach the threshold of undeniable responsibility for the perpetrator to get a punitive verdict against the offender. If prosecution to uphold international humanitarian law fails, the protection and deterrence International Humanitarian Law (IHL) provides evaporates over time. The legitimacy of these processes is also challenged if the lack of proper evidence leads to confusion and misunderstandings of who are the perpetrators – leading to arrests of innocent individuals for crimes
committed by others. Evidence gathering and evidence quality is pivotal for the success of the enforcement of IHL, and as a result the protection of human lives.

Intelligence gathering cyber operations is a tool that can be utilised to establish evidence gathering in an early stage of a conflict or violent ethnic cleavage as a digital humanitarian intervention. If humanitarian cyber operations are launched, it will gather information from network activity, wireless transmissions, cell phones, and other sources, utilising the rationale of humanitarian intervention. The benefits of humanitarian cyber operations are several, the humanitarian cyber operations can be quickly deployed, the humanitarian cyber operations can intervene on humanitarian ground early in a conflict and act as a deterrent against atrocities, and it is an option before deploying traditional military units.

**Humanitarian Intervention**

Military force can be justified under humanitarian intervention to intercept and prevent ongoing atrocities and to protect human lives. One example of humanitarian intervention is the landing of the US troops in Somalia in December 1992; others are the North Atlantic Treaty Organisation (NATO) bombings of Yugoslavia in 1999, and the military intervention in Libya 2011. Even if the concept of humanitarian intervention is debated and a matter of political cleavage, it is still accepted by the majority of the global community as a last resort to protect lives in civil wars and citizens of failing states.

Individual responsibility for war crimes is a concept that emerged after World War I. In a report to the International Peace Conference of 1919, the authors put forward evidence of war crimes by the Central Powers (Germany and Austro-Hungary). In the Versailles Treaty, individual responsibility for any atrocities was not addressed
and the responsibility to prosecute atrocities perpetrated by German officers resided with the Post-World War I Germany. The results of the German prosecution of the World War I war criminals seen with dissatisfaction by the Allies, as German war criminals was not held properly accountable. At the end of the World War II, the Allies decided to ensure that the Nazi perpetrators were held accountable. The International Military Tribunal, also called the Nuremberg Trials, held from November 1945 to October 1946, where the leading 24 Nazi leaders were put to trial. The Nuremberg Trials is the starting point for modern prosecution of crimes against humanity, which has developed through precedence and international agreements to an IHL codification.

From 1945 until today, the IHLs have built precedence and established a foundation for prosecution of war crimes and atrocities against the civilian population. The absence of evidence and witnesses is the major hurdle to overcome for the prosecution of war crimes. In the aftermath of the post-Yugoslavian Balkan wars the collection of evidence and securing witnesses, became especially difficult when the parties still existed after the war and refused to cooperate with the prosecution.

Humanitarian cyber operations would be active during the phase when a conflict is becoming violent towards non-combatant, based on the ability to act fast, and even be established pre-event in totalitarian regimes that already on a continuous basis utilising brute force against its own population.

**Using Cyber in a Humanitarian Role**

Perpetrators of atrocities expect in most cases not to be ever held accountable for their actions. The accountability of their actions disappears in the fog of war, turmoil, and societal chaos in civil wars and rapid regime changes. If the regime is stabilised by
fear and last for several decades, such as the Islamic Republic of Iran and the Soviet Union, the time passed will limit the ability to enforce laws and prosecute perpetrators. There are several reasons for this. Time will remove the strength of individual victim testimonies, public records disappear, and continued purges of opposition to the regime either leaves the potential witnesses dead or still alive but scattered all over the world as political refugees.

At the end of World War II the Swedish diplomat Raoul Wallenberg, together with the support of the staff of the post, was able to save thousands of Jews from the Nazi-occupied Hungarian capital Budapest, with one argument – accountability. The II World War was coming to an end, and Wallenberg was able to convince several high-ranked Nazis, and Hungarian henchmen to the Nazis, that it was a matter of time before they were in the hands of the Allies. Raoul Wallenberg changed the behaviour for several Nazi officials that executed the Holocaust, and Hungarians that collaborated with the Holocaust, by introducing the notion that the perpetrators would be personally liable at the end of the war. In Raoul Wallenberg’s negotiations with the perpetrators, he made it clear that the victors would not oversee with the crimes already committed by the perpetrators, but if they changed their behaviour and collaborated with Wallenberg’s campaign to save the Jews it could be used in the henchmen’s defence. Accountability matters. Not every Nazi or their collaborators accepted the argument, but enough to save thousands of Jews from a certain death. The rest of the Jews saved by Wallenberg were saved by bribes.

In the Islamic Revolution, 1979 in Iran, thousands of former Shah-loyalists and Marxists, and others that did not fit the new regime, were executed. After theocratic regime was established, Khomeini and after his death the new leaders continued to
arrest, persecute, and execute royalists, Jews, Baha’is, Marxists, Maoists, Mujahidin, Kurds, and apolitical youth that had triggered the anger of the regime. This repression of any deviance to the official way of life exists still in Iran.

The Iranian regime has committed repeated and serious atrocities against its own population, especially the minorities thereof, and the arrests, beating, and killing of these citizens are made by loyalists to the regime that are either devout to the ideology, benefit from the positions, or both. These perpetrators are acting on behalf of the regime, but that does not remove their personal accountability and times have changed in favour of evidence gathering.

In the year 2013, there were in the Islamic Republic of Iran 65 million cell phone users covering 84 per cent of the population, up from 1.46 per cent in year 2000. Approximate 31.4 per cent of all Iranians used the Internet in the year 2013. In the last decade the digital footprint has grown dramatically. Digital footprint is an information gathering opportunity. The increasing abundance of digital traffic from totalitarian regimes provides insights in their informal order structures, the way henchmen correspond to signalling from the elite, and how the inner-workings of a repressive regime is leading to actual crimes against humanity.

Humanitarian cyber operation can link the pieces together – perpetrator and event – and establish evidence that can be utilised for crimes against humanity prosecution later after the regime falls or the perpetrator can be apprehended. This evidence will be strong because humanitarian cyber operation can capture the casual chain from the regime’s elite to the actual execution of these orders, a linkage, a set of witnesses at the actual event cannot provide. Recent technological developments strengthen the case for humanitarian cyber operations.
The first decade of the War on Terror created new tools to support intelligence gathering and especially accumulated by open sources, digital transmissions, and intercepting wireless communications. The ability to track a Person of Interest (POI) over time, geospatial moves, through different technologies, and merge it as a unified profile was an achievement during the War on Terror. The tracking was supported by all forms of intelligence gathering, processed by advanced algorithms and reviewed by human analyst; leading to several major breakthroughs in tracking terrorist’s activity. The combined increased digital footprint from totalitarian regimes and the ability to track a Person of Interest (POI) over time, space, and communication channels would enable humanitarian cyber operations to operate under humanitarian intervention rules inside the networks of these totalitarian and repressive regimes. The strength of the investment in massive data mining has a natural humanitarian role.

In relation to these states the traditional Westphalian sovereignty matter, until the point where it can be verified that crimes against humanity are made, and then it would enable a digital humanitarian intervention utilising humanitarian cyber operations.

**Cyber as Deterrence against Atrocities**

The range in which military interventions are justified are limited for several reasons, such as the risk of escalation, inability to reach the intended goals by traditional military means, and the embedded concern of being a part of a larger conventional conflict beyond the scope of the humanitarian mission. Humanitarian cyber operations is a policy option, another tool set, that complement and support diplomacy, military
humanitarian intervention, and international cooperation in the pursuit of avoiding crimes against humanity.

A digital humanitarian intervention can be conducted openly, supported by international law, and then cyber operations can act as a deterrent against these crimes. The humanitarian cyber operations will limit the control and effectiveness of regime decisions in the totalitarian regimes due to the uncertainty of what is captured and evidenced by the humanitarian cyber operations.

Even if the totalitarian regime guarantees the confidentiality and integrity of the data and communications in their networks, it is unlikely that it is trusted as safe when a potential perpetrator assess the risks to be caught for crimes against humanity. Humanitarian cyber operations increases the uncertainty of future accountability and establishes that perpetrated deeds can be evidenced and captured through different channels, of which the majority is out of the control of the potential perpetrator.

The humanitarian cyber operations will then change the perceived risk and limit, and hopefully outweigh the perceived personal gain for the perpetrators and collaborators to the atrocities. Many actors in the staging of atrocities are ideologically or ethnically driven, and might not correspond to the threat of accountability, but even if a fraction corresponds to the threat of accountability it will have a sizeable impact and protect potential victims. Once these perpetrators prioritise their own personal future, logically they are more likely to collaborate with future investigations and act as witnesses, to the acts of those who ignored the increase risk for being held accountable.
Conclusion

Humanitarian cyber operations, and humanitarian cyber intervention, provide a new set of options and tools for decision makers in states that seek to uphold international human law and protect the life and liberty of fellow humans at risk. Humanitarian cyber operations are compared to traditional military deployment of conventional forces and airborne assets quickly deployed, and can provide assessments of the actual level of persecution and crimes against humanity either staged, planned, or ongoing, which enables the world community to act faster and with tangible evidence at hand.


4 Justice Lawrence, ‘The Nuremberg Trial,’ *International Affairs* (Royal Institute of International Affairs 1944-) 23(2), 1947, pp. 151-159.

