Strategic Analysis

ISSN: 0970-0161 (Print) 1754-0054 (Online) Journal homepage: http://www.tandfonline.com/loi/rsan20

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

Jan Kallberg

**To cite this article:** Jan Kallberg (2015) Bringing Fear to the Perpetrators: Humanitarian Cyber Operations as Evidence Gathering and Deterrence, Strategic Analysis, 39:4, 423-427, DOI: 10.1080/09700161.2015.1047226

**To link to this article:** http://dx.doi.org/10.1080/09700161.2015.1047226

*Strategic Analysis*, 2015
Vol. 39, No. 4, 423–427, http://dx.doi.org/10.1080/09700161.2015.1047226





*Commentary*

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

Jan Kallberg

## 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 state's national sovereignty.

Another advantage of 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 to hold those who perpetrate atrocities against civilians accountable, is secured unquestionable evidence.[1] The quest to secure evidence in the fog of war and the turmoil of modern conflicts is a challenging task. In the chaos of civil wars and ethnic conflicts, evidence is 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 the prosecution fails to uphold international humanitarian law (IHL) fails, the protection and deterrence provided by IHL evaporates over time. The legitimacy of these processes is also challenged if the lack of proper evidence leads to confusion and misunderstanding about who the perpetrators are, leading to arrests of innocent individuals for crimes committed by others.[2] Evidence gathering and evidence quality are pivotal for the success of the enforcement of IHL, and as a result the protection of human lives.

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

Dr. Jan Kallberg is a researcher at the Cyber Operations Lab, Cyber Security Research and Educational Institute, University of Texas at Dallas and part-time faculty at George Washington University.

## 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 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 in 2011. Even if the concept of humanitarian intervention is debated and a matter of political cleavage,[3] it is still accepted by the majority of the global community as a last resort to protect lives in civil wars and to protect 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 post-World War I Germany. The results of the German prosecution of World War I war criminals were viewed with dissatisfaction by the Allies, as German war criminals were not held properly accountable.[4] At the end of World War II, the Allies decided to ensure that the Nazi perpetrators were held accountable. The International Military Tribunal, also called the Nuremberg Trials, was held from November 1945 to October 1946, and the leading 24 Nazi leaders were put on trial. The Nuremberg Trials were 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, IHLs have built precedence and established a foundation for prosecution of war crimes and atrocities against civilian populations. The absence of evidence and witnesses is a major hurdle to overcome in the prosecution of war crimes.[5] In the aftermath of the post-Yugoslavian Balkan wars, the collection of evidence and securing witnesses became especially difficult as the parties still existed after the war and refused to cooperate with the prosecution.

Humanitarian cyber operations could be actived early when a repressive regime starts to use violence towards its own population and other non-combatant. The humanitarian cyber operations are faster to active and organize than traditional military means. If a repressive regime repeatly and consistent use force and repressive violent actions against civilians then foreign humanitarian cyber operations towards the totalitarian state are justified as a responsibility to protect under UN doctrine.

## Using cyber operations in a humanitarian role

Perpetrators of atrocities expect in most cases never to be held accountable for their actions. The accountability for 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 lasts 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 will disappear and continued purges of opposition to the regime either leave the potential witnesses dead or scattered all over the world as political refugees.

At the end of World War II the Swedish diplomat Raoul Wallenberg, with the support of the Swedish diplomatic staff in Budapest was able to save thousands of Jews from the

Nazi-occupied Hungarian capital Budapest, with one argument: accountability. World War II was coming to an end, and Wallenberg was able to convince several high-ranking Nazis and Hungarian henchmen that it was only a matter of time before they fell into the hands of the Allies. Raoul Wallenberg changed the behaviour of several Nazi officials that executed the Holocaust, and Hungarians that collaborated with them, 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 overlook the crimes already committed by the perpetrators, but if they changed their behaviour and collaborated with Wallenberg's campaign to save the Jews, this could be used in the henchmen's defence. Accountability matters. Not every Nazi or collaborator accepted the argument, but enough did to save thousands of Jews from certain death. The rest of the Jews saved by Wallenberg were saved by bribes.

In the Islamic Revolution of 1979 in Iran, thousands of former Shah loyalists and Marxists, and others that did not fit the new regime, were executed. After a 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.[6] This repression of any deviance from the official way of life still exists in Iran.

The Iranian regime has committed repeated and serious atrocities against its own population, especially the minorities thereof, and the arrests, beatings and killing of these citizens are carried out by those loyal to the regime who 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 2013, there were 65 million cell phone users in the Islamic Republic of Iran, covering 84 per cent of the population, up from 1.46 per cent in the year 2000. Approximately 31.4 per cent of all Iranians used the internet in the year 2013.[7] In the last decade the digital footprint has grown dramatically. The digital footprint is an information-gathering opportunity. The increasing abundance of digital traffic from totalitarian regimes provides insights into their informal structures, the way henchmen respond to signals from the elite, and how the inner workings of a repressive regime are leading to actual crimes against humanity.

Humanitarian cyber operations can link the pieces together—perpetrator and event—and establish evidence that can be utilised in prosecution of crimes against humanity later on, after the regime falls or the perpetrator has been apprehended. This evidence will be strong because humanitarian cyber operations can capture the causal chain from the regime's elite to the actual execution of their orders, a linkage that 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, especially accumulated from 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 merging 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 analysts, leading to several major breakthroughs in tracking terrorist activity. The combined increased digital footprint from totalitarian regimes and the ability to track a 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 matters, until the point where it can be verified that crimes against humanity are committed, and then it would enable a digital humanitarian intervention utilising humanitarian cyber operations.

## Cyber operations as deterrence against atrocities

The range in which military interventions are justified is limited for several reasons, including the risk of escalation, the inability to reach the intended goals by traditional military means, and the embedded concern of being part of a larger conventional conflict beyond the scope of the humanitarian mission. Humanitarian cyber operations are a policy option, another tool set, that complements and supports 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. Humanitarian cyber operations would limit the control and effectiveness of regime decisions in totalitarian regimes due to the uncertainty about what they can capture and evidence.

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 assesses the risks of being caught for crimes against humanity. Humanitarian cyber operations increase the uncertainty about future accountability and establish that perpetrated deeds can be evidenced and captured through different channels, the majority of which are outside the control of the potential perpetrator.

Humanitarian cyber operations will then change the perceived risk and limit, or 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 respond to the threat of accountability, but even if a fraction responds to the threat of accountability it will have a sizeable impact and protect potential victims. Once these perpetrators prioritise their own personal futures, logically they are more likely to collaborate with future investigations and act as witnesses to the acts of those who ignored the increased risk of 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 quickly deployed compared to traditional military deployment of conventional forces and airborne assets, 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.

**Disclosure statement**

No potential conflict of interest was reported by the author.

**Notes**

1. Stephanos Bibas and William W. Burke-White, 'International Idealism Meets Domestic-Criminal-Procedure Realism',*Duke Law Journal*, 59, 2009, p. 637.
2. Katie Zoglin, 'The Future of War Crimes Prosecutions in the Former Yugoslavia: Accountability or Junk Justice', *Human Rights Quarterly*, 27(1), 2005, pp. 41–77.
3. Didier Fassin and Mariella Pandolfi, *Contemporary States of Emergency: The Politics of Military and Humanitarian Interventions*, Zone Books, New York, 2010.
4. Justice Lawrence, 'The Nuremberg Trial', *International Affairs* (Royal Institute of International Affairs 1944–), 23(2), 1947, pp. 151–159.
5. Gary Jonathan Bass, *Stay the Hand of Vengeance: The Politics of War Crimes Tribunals*, Princeton University Press, Princeton, NJ, 2014, p. 226.
6. Ervand Abrahamian, *Khomeinism: Essays on the Islamic Republic*, University of California Press, Oakland, CA, 1993.
7. International Telecommunication Union (ITU), at http://www.itu.int/net4/itu-d/icteye/ (Accessed March 12, 2015).