Geneva Conventions for Cyber Warriors Long Overdue

Cyber warfare is a fact of the modern world. However, there is no clear international law that distinguishes between warfare, terrorism, crime or vandalism. As a result, U.S. military cyber warriors are operating without the protections and restrictions their kinetic brethren enjoy under the Geneva Conventions.

The road to those agreements was long, but necessary and it needs to be trod again — before civilians suffer the consequences of unrestricted cyber warfare.

In the last decade, U.S. and international leaders have recognized the military implications of the growing threat. The United States established Cyber Command in 2009 and the Navy stood up the 10th Fleet in 2010 to direct cyber operations and defense. Ret. Adm. James Stavridis, the supreme allied commander for Europe and commander of NATO from 2009 to 2013, argued further for a separate service branch, a cyber force. However, a U.S. cyber force would be a service branch and combatant with no directly applicable international law of warfare.

After years of study, NATO only applies pre-cyber era international law to cyber operations, both conducted by and directed against states.

In 2008, NATO established the Cooperative Cyber Defence Centre of Excellence, originally proposed by Estonia following a growing awareness of the vulnerability of NATO allies and partners to cyber attack, particularly by Russia. In 2009, the center hosted a conference in Tallinn, Estonia, with 20 international experts — almost exclusively from NATO countries — to seek a way to apply existing industrial-age international law to cyber warfare, resulting in the *Tallinn Manual*. While a laudable attempt to make progress, Russia has yet to endorse the NATO-developed rules on many issues but the *Tallinn Manual* process continues.

After every great war, there have been calls to ameliorate its new horrors. Can the United States and other developed nations see the potential danger of cyber warfare enough to contain it before a cyber Dresden? During World War II, the Allies bombed the war industry, railroad and communications center in the German city of Dresden. The incendiary attack of valid military targets resulted in massive collateral damage and over 20,000 dead. At that time, the most recent Geneva Convention had been signed in 1929, extending protections of soldiers and sailors in battle to prisoners of war. Air warfare had not yet been covered in spite of the experiences of World War I.

The world was horrified by the human catastrophe of World War II, particularly the massive civilian devastation from strategic bombing — the ultimate forcing function to draft international law protecting civilians in armed conflicts in addition to protecting servicemen. Conventions were added outlawing chemical warfare, biological warfare and anti-personnel mines, and outlining protocols to address guerilla and civil warfare, but not yet cyber warfare.

While some international law may be applicable, the remaining ambiguity on cyber warfare leaves individuals and organizations vulnerable. NATO's original founding treaty, designed to safeguard the freedom of member states, identified the trigger for a collective response in Article 5 as "an armed attack against one or more of them in Europe or North America." NATO Article 5 protection may be applied against a cyber attack, but has not been yet.

Nations, rebels and guerillas know the difference between a legitimate military target and a hospital, but cyber warfare has no bounds. Responding to insurance claims for the NotPetya attacks, a global professional services firm Marsh & McLennan created a three-factor standard to determine if a cyber attack is an act of war and could be excluded from payment, based on the effects, the victims and the purpose of the attack. By that standard, uniformed Russian military hackers could shut down the New York Stock Exchange and NASDAQ for a month and not consider it an act of war.

While some confuse cyber operations with information warfare, they are different. The U.S. Military Universal Joint Task List is a common language which serves as the foundation for joint operations planning across the range of military and interagency operations. The list defines "Coordinate Offensive Cyberspace Operations" as a separate and distinct task from "Coordinate Strategic Information Operations." Offensive cyber is "the application of force in and through cyberspace. [It] may target adversary cyberspace functions or use first-order effects in cyberspace to initiate cascading effects into the physical domains." On the other hand, information operations are "the integrated employment of … electronic warfare, military deception, and operations security, in concert with … cyberspace operations and public affairs."

Any international law or future convention must recognize such distinctions.

Even with the existing definitions around cyber operations and the damage caused by cyber attacks to date, both the public and private sector have failed to identify and act upon a tangible solution to existing threats. Books on the trauma of cyber warfare are plentiful because the risks to individuals are real and immediate. Cyber attacks threaten all forms of critical infrastructure and governmental service institutions, including power grids, police and hospitals.

During 2017, even state legislatures became concerned about the cybersecurity of U.S. elections. The City of Baltimore was held hostage for months by a ransomware attack, which raises several concerns considering a ransomware attack on only one major city the day of a presidential election could flip the outcome of a state and the nation.

Industry is so concerned that Microsoft's president and chief legal officer took a bold step proposing a "Digital Geneva Convention" and outlined such a protocol as the urgent threat of cyber warfare is discussed around the world.

The complications remain monumental. Not only have the UN and other groups failed to reach consensus, but they are also arguably diverging because of the depth and breadth of the issue.

Further, while international governments fear the effects of cyber attacks, there is a clear lack of incentive for governments to disarm what some consider a critical offensive capability.

One of the advantages of cyber warfare is that it gives the president and combatant commanders an option short of kinetic warfare. Traditionally, U.S. leaders think of the national instruments of power in terms of diplomacy, information, military and economy, better known as DIME. There is something to be said for measures more effective than Twitter and economic sanctions, but less destructive than high explosives. After the Iranian Revolutionary Guard Corps shot down a U.S. Global Hawk drone, the expected response was to plan a massive kinetic reprisal. However, the president chose a cyber response instead. Other cyber attacks were reported to have slowed Iranian nuclear developments.

While U.S. cyber warfare is planned in a targeted, precise and surgical manner, less scrupulous practitioners have demonstrated the potential for collateral damage on a vast scale from a misdirected or errant attack.

Where governments have failed, an independent international group may be able to hammer out the basics of a convention on cyber warfare, if the right people come together with the right mindset and reasonable expectations. Business leaders and local officials could establish a framework with the help of international lawyers, under the expectation that when it was acceptable and politically necessary, diplomats would have to pick up the torch.

This is how the Red Cross completely replaced the Geneva Conventions after World War II.

Setting the conditions to negotiate a final diplomatic agreement acceptable to even 20 of 200 nations will require exceptional management and leadership. This is a design thinking exercise for a global problem: first create empathy, define the problem, ideate solutions, prototype answers and test them. The solution must be considerably more effective than a communique; it must hold the force of international law.

Protecting civilians from future cyber warfare is a lofty purpose when considering how difficult it would have been in 1910 for nations to predict the nature of submarine or air warfare by the end of World War I. In 2010, few could have comprehended the ubiquitous 2020 Internet of Things given the first iPhone was sold in 2007 and the World Wide Web had only been proposed in 1989.

France's President Emmanuel Macron launched an effort at the 2018 UNESCO Internet Governance Forum to address cybersecurity. It resulted in a strongly worded memo, the Paris Call for Trust and Security in Cyberspace, endorsed by 370 actors, including corporations, non-governmental organizations and nations.

An independent international organization supported by independent citizens and businesses can succeed with the help of international lawyers, where governments have failed.

Because cyber attacks do not draw blood, an international business association with global vision may be the more appropriate group to address the protection of civilians.

Defining belligerents may be radical. A great deal of literature contemplates the ethics and impact of governmental cyber warfare attacks on foreign civilian systems, but fails to consider the inverse: can Google commit an act of war? While it is unlawful to bomb a mosque, there is no law to prevent patriotic citizen hackers from launching a cyber attack.

Developing ethical solutions to questions like these will be unprecedented because of the complexity of modern society: could Amazon Web Services be considered a cyber combatant? There must be distinguishing factors between government contracts, criminal acts and casus belli — an act or event that provokes or is used to justify war — for a business.

Extending the Geneva Conventions to guerilla and civil wars, or non-international warfare, was not easy. Facebook might one day possess the power to initiate a civil war, just as Twitter users could evolve into a subversive guerilla force.

The post-World War II Geneva Conventions were only signed by 18 nations in 1949; the rest came slowly over decades. Given the high number of non-participating nations, even this example demands scrutiny around who must initially participate to succeed.

What are the cyber threats to individuals, businesses, or governments not already governed by treaty? Where would jurisdiction to resolve disputes rest? Who signs — France,

> "Can the United States and other developed nations see the potential danger of cyber warfare enough to contain it before a cyber Dresden?"

Vodaphone or Apple? Can entities distinguish between cyber crime, espionage, intelligence and attack?

Can a cyber convention establish rules that prevent cyber collateral damage? Would valid military cyber targets be required to mark themselves with a fixed distinctive sign to distinguish them from civilian targets?

The ICRC model can work again. This requires leaders to announce clear intent, inspire others to collaborate, create a first draft of a convention, revise and edit the articles, then bring social pressure to bear on governments to adopt a negotiated treaty. A preliminary conference gives the opportunity to identify the issues to address, then articles can be proposed and crafted for each at the convention.

The UN has failed, nations have failed, and corporations have failed while the trends in cyber warfare have been consistently if not exponentially negative. A cyber Pearl Harbor remains a threat and perhaps it is time to declare cyber a domain; it is certainly time to recognize that military personnel and civilians can all be gravely harmed by non-kinetic forces.

Failing to act leaves U.S. servicemen and women at risk: nothing stops a foreign nation from declaring the 10th Fleet "Yankee Cyber Pirates" and indicting them for cyber war crimes even in the absence of explicit international law. ND

Steve Waugh is acting chief scientist of the combat systems group at Johns Hopkins University's Applied Physics Lab.

iStock photo