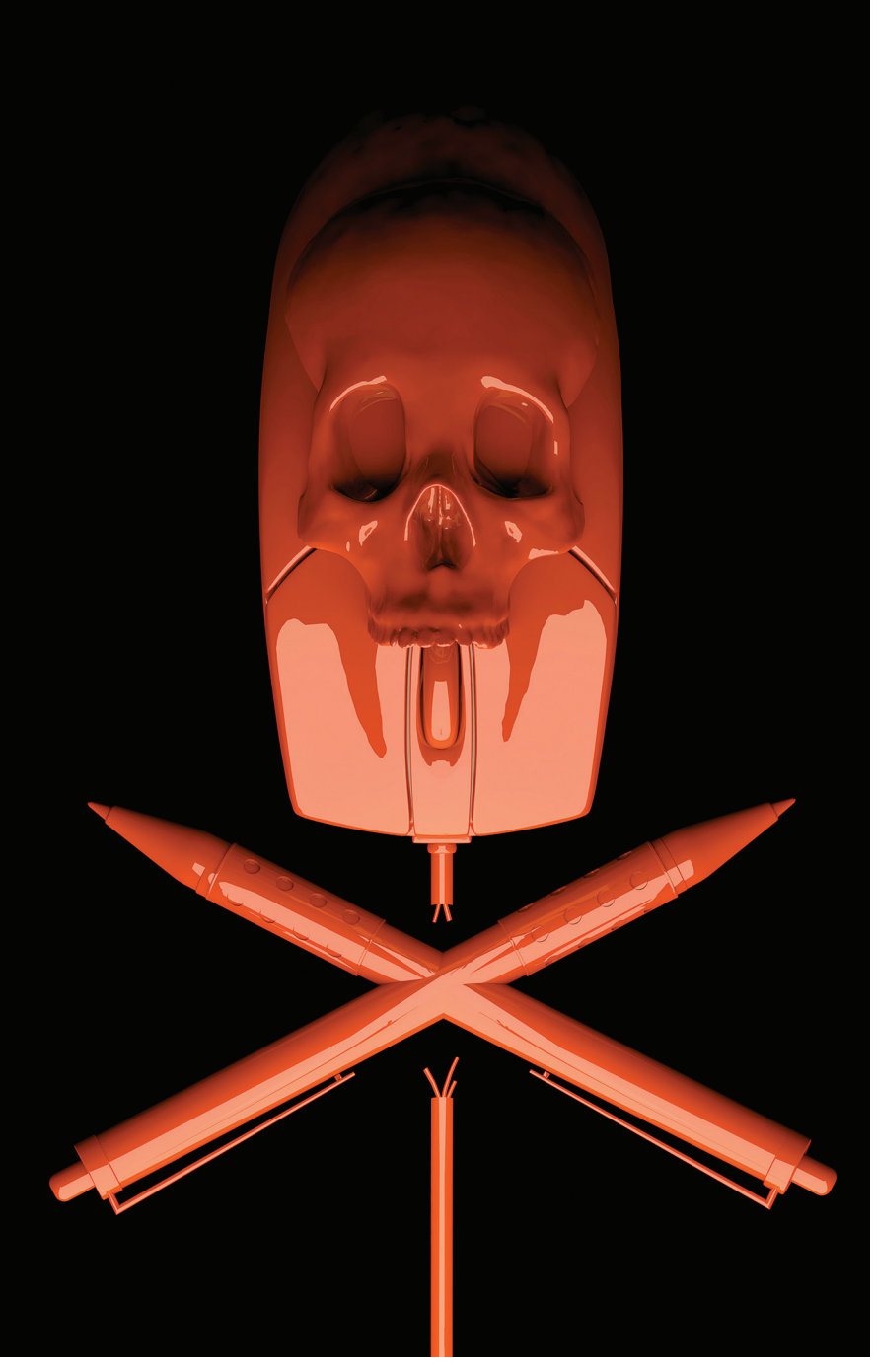

Writing the Rules of Cyberwar

The world needs a Geneva Convention for cyberspace

BY KARL RAUSCHER

IN THE 21ST CENTURY, just about everything is vulnerable to cyberattack. A hit on a bank or a stock exchange would cause uproar in the financial sector; a strike on an electrical grid could shut down a city. And the consequences of an attack could be far more dire than mere inconvenience. If hackers disrupted operations at a nuclear power facility, they could trigger a meltdown. An attack on a hospital could leave doctors scrambling in the dark, machines failing, and patients dying in their beds.

Such scenarios are becoming ever more plausible. In 2007 the cyberwar era began in earnest, when Estonia's government networks were hacked during a political dispute with Russia. In recent years, the United States and China have accused each other of sponsoring major cyberintrusions, and Iran has accused the United States and Israel of unleashing a worm against its nuclear installations. Before such activities escalate into cyberattacks that destroy innocent lives, we should apply the lessons of the bitter past and establish the norms of cyberconflict. We should define acceptable targets, and we could even place limits on cyberweapons, just as we did on chemical ones nearly a century ago.

I propose bringing the principles of the Geneva and Hague conventions to bear on cyberconflicts. These conventions, which reached mature form after the First World War, establish rules for the treatment of civilians, prisoners of war, and the wounded, and they also ban the use of certain weapons,

ILLUSTRATION BY Eddie Guy

such as poisonous gas. Preserving these principles is of solemn relevance to billions of people, yet there is still no clear way to apply them to cyberattacks. While it's unlikely that nations could be convinced to sign on to a legally binding treaty, international norms could have the same effect.

To find the way forward, the EastWest Institute has created the Cyber 40, with delegates from 40 digitally advanced countries. Our think tank specializes in back-channel negotiations between countries that don't normally cooperate, and I head the institute's Worldwide Cybersecurity Initiative. We have issued practical recommendations on spam and hacking, many of which have already been implemented. Since we presented our first proposal for "rules of the road" for cyberconflicts in a Russia-U.S. bilateral report at the 2011 Munich Security Conference, the ideas have gained traction. Other groups are also working on the legal issues surrounding cyberattacks—most notably a NATO-related collaboration based in Tallinn, Estonia, which published its findings this March as the *Tallinn Manual*.

In cooperation with industry groups and think tanks in China, Russia, and other countries, we are now trying to define practical humanitarian agreements for cyberconflicts. Such agreements could, for example, designate critical civilian infrastructures like hospitals and electronic medical records as off-limits for cyberattacks. And we hope to at least begin a conversation on whether some cyberweapons are analogous to weapons banned by the Hague and Geneva conventions as offensive to "the principles of humanity and the dictates of the public conscience."

Our international team has reviewed all 750 articles in the Geneva and Hague conventions, in each case asking whether the rule can be transferred directly from the physical world to the cyberworld. Often the situation is simpler in the material world: For example, the difference between routine intelligence gathering and warfare is relatively clear. In cyberoperations, the infiltration of a computer network could be espionage or the prelude to an offensive action—but the mechanism is the same in both cases.

Seemingly straightforward prohibitions, such as the one on attacking hospitals, become complicated when ported to cyberspace. In the physical world, military officials can easily distinguish between a hospital and an army base and can plan their campaigns accordingly. In the cyberworld, everything is intermingled. Hospital records may be stored on a server in a data center that may also store data from a military contractor. In fact, it is the ease with which data and data-searching functions can be distributed across networks that makes cyberspace valuable in the first place.

When we built the Internet, we weren't thinking about how to implement the Geneva Conventions online. To adapt these rules to our era, we must therefore model cyberconflicts, define legitimate targets, and suggest ways of determining compliance with such guidelines.

We will have to mark nontargets in some way. The Geneva and Hague conventions direct that protected entities (such as hospitals and ambulances) and protected personnel (such as medics) be marked in a clearly visible and distinctive way, for instance, with a red cross or red crescent. Marking a hospital's presence on readily available maps constitutes another such warning.

We've been conducting an assessment of special ways to designate protected humanitarian interests in cyberspace. We're currently working with our international partners to evaluate a number of technical solutions to this challenge. For instance, one early idea was to use ".+++" to mark the Internet addresses of hospitals and health databases.

Of course, merely marking protected zones in cyberspace would not stop miscreants from barging into them; then again, neither does the presence of a Red Cross symbol cause a bomb to bounce off a medical clinic. The point is that such markers would allow a state that wanted to comply with the norm to write virus code or arrange attacks so as to avoid designated institutions.

ASSUMING WE CAN DEVISE A SYSTEM to create safe havens on the Internet, another concern is how to get all the necessary parties involved. In the past, the rules of war could gain force if the major nation-states agreed to them. That's not enough to ensure the usefulness of cyberconflict rules, however, because cyberwarriors may be nonstate actors, sometimes even individuals. In order to get those people to respect the rules, we'll need all the world governments to come together to condemn certain acts. Such a consensus would carry enough moral force to isolate any cyberwarriors who cross the line.

I first thought about this question while serving on the National Security Telecommunications Advisory Committee for President George W. Bush. In 2002, when our group met with Vice President Dick Cheney at the White House, one member of the committee asked Cheney which countries the United States should engage with on questions of cybersecurity. His first answer was obvious: the anglophone countries that were eager to partner with us. "But the second answer will really surprise you," he said. We never heard it. At that moment, the Secret Service descended on him and whisked him, and us, away to safety. It was all because of a false alarm that sounded when a small Cessna plane accidentally breached restricted airspace over the White House.

Ever since, I have wondered what Cheney's second suggestion would have been—and my life's work has come down to an attempt to find my own answer. I've come to the conclusion that we have to work with the difficult countries because those are the countries that matter. "Difficult countries" will mean different things to different countries; for the United States, though, the list would surely include Russia and China, both of which are formidable for their technological prowess.

The EastWest Institute's Worldwide Cybersecurity Initiative has therefore begun bilateral processes with experts

We could place limits on cyberweapons, just as we did on chemical weapons nearly a century ago

from the United States and Russia to define the terms used in discussions of cyberconflicts, so that future negotiators will have a clear dictionary to help them differentiate between, for example, cybercrime and cyberterrorism.

We have also brought U.S. and Chinese experts together to produce joint recommendations for fighting spam and botnets—the networks of hijacked computers that are used in some attacks. These recommendations were adopted by the Messaging, Malware, and Mobile Anti-Abuse Working Group, which brings the world's biggest Internet companies together to swap strategies and collaborate on projects. Most recently, we've worked with our Chinese counterparts to issue recommendations on how to resolve conflicts over hacking. With these efforts, we've prepared the way for extending the humanitarian principles of the Geneva and Hague conventions into cyberspace.

IT HAS SOMETIMES been argued that international norms are toothless—that countries resort to chemical and biological attacks rarely only because they fear facing retaliation in kind. However, recent events in Syria's civil war show that norms do matter. The Syrian government, which is not party to the Chemical Weapons Convention, nevertheless felt the world's wrath when it allegedly used poison gas against rebel forces and civilians. The United States first threatened to intervene in the war to protest the action. However, that threat was revoked when the regime's allies—notably Russia, which was on record as opposing chemical warfare—devised a plan to take away Syria's chemical weapons.

This case illustrates some of the problems that would face any attempt to enforce the norms of cyberwarfare, most obviously the problem of tracing an attack to its perpetrator. The Syrian government maintained that it had not broken international laws against chemical warfare, and some observers agreed that it wasn't completely clear who had done the deed. It could even have been a provocation or, perhaps, a blunder on the part of the rebel commanders. Happily, the international community was able to agree on a practical remedy despite the lack of hard proof.

If we can set the parameters of basic human decency in time of cyberwar, then maybe we can ban aspects of such warfare altogether. At the least, we can discuss taking some cyberweapons off the table. Some of them do, after all, carry the potential for viral behavior, with a lack of discrimination regarding targets, and they all travel at computer speeds. These attributes, combined with a belligerent cause, are an understandable reason for concern.

We can bring the principles of the Geneva Conventions into the 21st century if we agree that these rules are worth preserving and agree that war need not be the infliction of maximum suffering on the enemy. Some may call me naive, but I believe mankind can be civilized even as we engage in a new era of cyberconflicts. ■

POST YOUR COMMENTS at http://spectrum.ieee.org/cyberwar1213

ESPIONAGE, SABOTAGE, AND MORE

In the past decade, cyberattacks have changed from theoretical concerns to urgent national priorities. While the bulk of attacks target private companies for economic gain, here's a roundup of attacks that may have been launched with political intent.

STUXNET TARGET: Iran's Bushehr nuclear power plant took a hit.

2007 In Estonia, the websites of some government agencies, financial institutions, and newspapers are shut down by **denial-of-service attacks** during a political spat with Russia.

2008 During the run-up to the U.S. presidential election, e-mails containing **malware** are sent to top aides in the campaigns of both Barack Obama and John McCain, and internal position papers and e-mails are accessed. The U.S. government blames foreign hackers.

2008 In the weeks before the Russia-Georgia war, Georgia's Internet infrastructure and some government websites are hit with a **denial-of-service attack**.

2009 In a vast spy campaign known as **GhostNet**, e-mails containing malware are used to take control of computers in dozens of embassies, foreign ministries, and Tibetan exile centers around the world. The researchers who discover GhostNet believe it's controlled by Chinese networks.

2010 Iran's nuclear facilities are sabotaged by the **Stuxnet** worm in one of the first uses of offensive cyberweapons. During an investigation by *The New York Times*, many unnamed officials say that the United States and Israel created the worm.

2010 One month after the websites of many Pakistani government ministries are **shut down and vandalized**, with Indian hacker groups claiming credit, the websites of Indian security agencies are similarly attacked by Pakistani hackers.

2011 The Canadian government has to disconnect its two main economic agencies from the Internet when a **computer virus** sweeps through government networks, seeking out classified documents and sending them back to hackers. The attacks are traced as far back as computer servers in China.

2012 A malware program known as **Flame** is discovered in computers across the Middle East, with the majority of targets in Iran. The sophisticated cyberespionage program shares some source code with Stuxnet but is described by experts as being far more complicated.

2013 Operations at several South Korean television stations and major banks are disrupted when a malware program known as **DarkSeoul** renders computers unusable. Many experts speculate that North Korea is responsible.