foreignpolicy.com

In Cyberwar, There are No Rules

Tarah Wheeler

23-29 minutes

In 1984, a science fiction movie starring an up-and-coming Austrian-American actor took the box office by storm. A cybernetic organism is sent back in time to seek out and kill the mother of a great war hero to prevent his subsequent birth. The cyborg scans a phone book page and begins methodically killing all women named Sarah Connor in the Los Angeles area, starting at the top of the list.

If *The Terminator* were set in today's world, the movie would have ended after four and a half minutes. The correct Sarah Connor would have been identified with nothing but a last name and a zip code—information leaked last year in the massive Equifax data breach. The war against the machines would have been over before it started, and no one would have ever noticed. The most frightening thing about cyberwarfare is just how specifically targeted it can be: An enemy can leap national boundaries to strike at a single person, a class of people, or a geographic area.

Nor would a cyborg be necessary today. According to U.S.

census data, there are currently 87 people in the United States named Sarah Connor. Many of them probably drive cellular-enabled cars that run outdated firmware, use public unencrypted Wi-Fi, and visit doctors who keep unsecured health care records about patient allergies and current medications on computers running the infamously outdated and vulnerable Windows XP operating system.

These days, warfare is conducted on land, by sea, in the air, across space, and now in the fifth battleground: cyberspace. Yet so far, the U.S. government has fumbled on cybersecurity, outsourcing much of that area of conflict to the private sector in accordance with the Trump administration's most recent National Security Strategy—leaving the country exposed to foreign attack.

Those third parties operate under exactly the same incentives as any pharmaceutical company. If a company's service is the treatment of symptoms, preventive medicine is a threat to its business model. Meanwhile, pundits, policymakers, and publishers take as gospel what they're told by so-called cybersecurity experts who have more social media followers than relevant credentials in the field, which is how hysterical "The Hackers Are Coming for Us" editorials find their way into otherwise respectable publications.

Increased fear, uncertainty, and doubt surrounding cybersecurity have led to a world where we cannot tell what has and hasn't happened. The nature of cyberwarfare is that it

is asymmetric. Single combatants can find and exploit small holes in the massive defenses of countries and country-sized companies. It won't be cutting-edge cyberattacks that cause the much-feared cyber-Pearl Harbor in the United States or elsewhere. Instead, it will likely be mundane strikes against industrial control systems, transportation networks, and health care providers—because their infrastructure is out of date, poorly maintained, ill-understood, and often unpatchable. Worse will be the invisible manipulation of public opinion and election outcomes using digital tools such as targeted advertising and deep fakes—recordings and videos that can realistically be made via artificial intelligence to sound like any world leader.

The great challenge for military and cybersecurity professionals is that incoming attacks are not predictable, and current strategies for prevention tend to share the flawed assumption that the rules of conventional war extend to cyberspace as well. Cyberwarfare does have rules, but they're not the ones we're used to—and a sense of fair play isn't one of them. Moreover, these rules are not intuitive to generals versed in fighting conventional wars.

That's a problem because cyberwar won't be waged with the informed participation of much of the U.S. technology sector, as the recent revolts at Google over AI contracts with the U.S. Defense Department and at Microsoft over office software contracts with U.S. Immigration and Customs Enforcement

demonstrate. That leaves only governments and properly incentivized multinational corporations to set the rules. Neither has yet provided a workable and operational definition of what constitutes a globally recognized act of war—a vital first step in seeking to prevent such transgressions.

The closest that the U.S. military has come to such a definition is to say that "acts of significant consequence" would be examined on a case-by-case basis and could require congressional evaluation. But given how quickly a cyberattack could disable critical infrastructure, expecting Congress to react in time to answer effectively is unrealistic.

In a world where partisan politics have been weaponized, a smart misinformation campaign by a foreign state that targeted only one political party might even be welcomed by other parties so long as there was plausible deniability—and with cyberattacks, attribution is rarely certain.

There is also a serious risk of collateral damage in cyberoperations. Most militaries understand that they are responsible not only for targeting strikes so that they hit valid targets but also for civilian casualties caused by their actions. Though significant collateral damage assessment occurs prior

to the United States authorizing cyberoperations, there is no international agreement requiring other powers to take the same care.

A major cyberattack against the United States in 2014 was a clear example of how civilians can bear the brunt of such operations. Almost all cybersecurity experts and the FBI believe that the Sony Pictures hack that year originated in North Korea. A hostile country hit a U.S. civilian target with the intention of destabilizing a major corporation, and it succeeded. Sony's estimated cleanup costs were more than $100 million. The conventional warfare equivalent might look like the physical destruction of a Texas oil field or an Appalachian coal mine. If such a valuable civilian resource had been intentionally destroyed by a foreign adversary, it would be considered an act of war.

In the near future, attacks like the Sony hack will not be exceptional. There are countless vulnerabilities that could result in mass casualties, and there are no agreed norms or rules to define or punish such crimes. Consider the following examples.

Once a week, a European aircraft manufacturer cleans all plane cockpits of Android malware. Pilots can pass malware to the plane from their smartphones when they plug them in, which the plane (while theoretically unaffected by phone-only malware) then passes it on to the next pilot with a smartphone. Planes are already covered in viruses, both

virtual and microbial. In such a vulnerable environment, even an unsophisticated hack could wreak havoc. A text message sent to the phone of every in-air pilot giving them a national security warning or rerouting their planes could lead to emergency landings and widespread confusion, with more sophisticated attacks potentially leading to far more serious consequences.

Aviation is not the only vulnerable sector. The U.S. health care system is full of medical devices running ancient firmware or operating systems that simply cannot be patched or hardened against commonly known network intrusions. Small hospitals often cannot afford to replace their medical equipment on a regular schedule, and device providers may deprioritize or block security patches or upgrades in order to sell updated devices in the next round of production.

That's a problem in an era when many surgical procedures are assisted by robots, which hospitals struggle to keep secure. The medical device industry focuses more on performance and patient health outcomes than on keeping a cyberadversary at bay. A cyberattack on hospitals using robotic surgical devices could cause them to malfunction while in use, resulting in fatal injuries. If a country or terrorist group decided to take out a sitting U.S. senator undergoing robotically assisted surgery and then covered its tracks, the perpetrator's identity would be hard to pinpoint, and there would be no clear U.S. legal precedent for classifying the

hacking of hospital equipment as an assassination or an act of war. Nor do there appear to be clear protocols for retaliation.

There are less direct potential vectors of attack, too. Recently, a cold storage facility for embryos in Cleveland failed to notice that a remotely accessible alarm on its holding tanks had been turned off, leading to the loss of more than 4,000 frozen eggs and embryos. Many operators of industrial control systems never bother to change all their default passwords or security credentials, which can leave them vulnerable to ransomware attacks, and even fewer health care officials are likely to assume that someone might deliberately shut off sensors that monitor the viability of future human life. It is difficult to determine whether the Cleveland eggs and embryos were lost due to a simple maintenance failure or deliberate tampering—but as techniques such as the freezing of eggs become more common in wealthy nations, such a simple attack could wipe out thousands of future citizens.

There is no functional difference between a foreign soldier taking an ax to refrigerant tanks to destroy 4,000 eggs and embryos and that same soldier using a keyboard to remotely shut down the facility's temperature maintenance protocols from 6,000 miles away. The two acts are equally heinous on a moral level. The uncertainty in attribution and the lack of an easily identified villain may make the latter seem the province of science fiction. But it is not.

Cyberattacks—some egregious, some mundane—are happening now, quietly and unnoticed by the public. Much of the confusion and fear over cybersecurity comes from the distorted publicity surrounding a few outlying events. While cybersecurity experts can't have perfect certainty over attribution or even the existence of some attacks, we can understand the larger security landscape, in which cybersecurity is merely a banal and predictable component of national infrastructure. The risk of cyberattacks is knowable, probabilistically.

Technology and cyberspace are changing faster than countries can legislate internally and negotiate externally. Part of the problem with defining and evaluating acts of cyberwarfare against the United States is that U.S. law is unclear and unsettled when it comes to defining what constitutes an illegal cyberact as opposed to normal computer activity by information security researchers.

The legal status of most information security research in the

United States therefore remains unclear, as it is governed by the poorly drafted and arbitrarily enforced 1986 Computer Fraud and Abuse Act (CFAA)—a piece of legislation that was roundly derided by tech experts on its inception and has only grown more unpopular since. The law creates unnecessary fear that simple and useful information security research methods could be maliciously prosecuted.

These methods include network scanning using tools such as Nmap (a computer network discovery and mapping tool) or Shodan (a search engine for devices on the internet of things) to find unsecured points of access to systems. Such scanning does not constitute the exploitation of computer or network vulnerabilities; a real-world equivalent would be walking down a street and noting broken windows, open doors, and missing fence planks without actually trespassing on someone else's property. One of the fastest fixes for the dismal state of federal cybersecurity expertise would be to overturn the CFAA and reward cybersecurity researchers engaged in preventive research instead of tying their hands with fears of breaking the law. Yet at present the U.S. government ham-handedly discourages many information security researchers from entering what should be a noble service.

This dynamic has left the U.S. government with critical shortfalls in top-level information security experts. The United States simply lacks a viable legislative plan for hardening its infrastructure against cyberattacks and developing much-

needed cybertalent. Any strong defense against cyberattacks should follow the same principles used for basic U.S. infrastructure design: strategists plan, technicians execute, and experts examine. For example, the interstate highway system in the United States, authorized in 1956 to enable rapid military transport of troops and supplies, also had much broader civilian benefits.

Now, through neglect, roads in the United States are riddled with potholes, widening cracks, and crumbling asphalt; thousands of deaths on U.S. highways per year are related to poor road conditions. Yet potholes are the most boring problem imaginable for a policymaker. By contrast, whenever a bridge collapses, it grabs headlines—even though a comparatively small number of people per year die from bridge catastrophes. Incident response is appealing; it lets policymakers show their leadership chops in front of cameras, smoke, and sirens. The drudgery of repairing underlying problems and preventing the disasters in the first place takes a back seat. This is dull but essential policy work, and the same goes for technology infrastructure. If cyberwork isn't boring, we're doing it wrong.

> The drudgery of repairing underlying problems and preventing the disasters in the first place takes a back seat. This is dull but essential policy work, and the same goes for technology infrastructure. If cyberwork isn't boring, we're doing it wrong.

> The drudgery of repairing underlying problems and preventing

> the disasters in the first place takes a back seat. This is dull but essential policy work, and the same goes for technology infrastructure. If cyberwork isn't boring, we're doing it wrong.

Cybersecurity should be akin to a routine vaccine, a line item in the infrastructure budget like highway maintenance. Basic cybersecurity measures—such as upgrades to encryption, testing the capability of recovery in the event of data loss, and routine audits for appropriate user access—should be built into every organizational budget. When incidents happen—and they will happen as surely as bridges collapse—they should be examined by competent auditors and incident responders with regulatory authority, just as major incidents involving airlines are handled by the National Transportation Safety Board (NTSB).

At present, however, the United States lacks an NTSB for cybersecurity. Due to the government's lack of expertise, it is overly reliant on large companies such as EY, PwC, and Deloitte to handle this work. If the U.S. government isn't capable of running a post-mortem on major cyberevents, citizens should be asking why—instead of letting lawmakers hand the work to contractors. Responding to major cyberattacks requires battalions of highly trained government analysts, not armies of accountants and attorneys.

Yet the White House, under President Donald Trump, has failed to fill or has outright eliminated almost every major cybersecurity position. There are a few brilliant holdouts

bravely providing solid advice on information security and best practices. (The government agency 18F and the United States Digital Service are both doing valuable work but receive far smaller budgets than they deserve.) But cybertalent is draining faster than it is being replaced at the highest levels.

Cyberdefense isn't magic. It's plumbing and wiring and pothole repair. It's dull, hard, and endless. The work is more maintenance crew than Navy SEAL Team 6. It's best suited for people who have a burning desire to keep people safe without any real need for glory beyond the joy of solving the next puzzle.

The challenge for policymakers is the same as it ever was: Improving lowest-common denominator infrastructure in cybersecurity makes for the most effective defense against ill-intentioned adversaries. Yet politicians have been slow to respond since there's little pork in password policies, and forcing everyone to improve their encryption takes a distant second place to kissing babies on the campaign trail.

When devastating attacks happen on U.S. soil, people use metonyms to describe them. No one has to describe the specifics of Pearl Harbor or 9/11; we already know what they signify. When the cyberattack that lives in infamy happens, it will be so horrifying that there won't be a ready comparison. It won't be the cyber-Pearl Harbor. It will have its own name.

Until that point, however, these attacks will remain nameless. People are frightened of what they can see and understand, not what they cannot imagine and do not comprehend, and, as a result, it's easy to ignore the twice-removed effects of a quiet but deadly cyberattack. Given that it took more than a decade and a half to successfully prosecute war criminals from the Yugoslav wars of the mid-1990s even with overwhelming photographic evidence and personal testimony, it's not surprising that the international community has a hard time agreeing on what constitutes a cyberattack deserving of reprisal—especially when countries can't even settle on a definition for themselves.

The first step to improving cyberdefense would be to determine what does, in fact, constitute a cyberattack by a foreign power as opposed to a mere prank or industrial espionage.

The first step to improving cyberdefense would be to determine what does, in fact, constitute a cyberattack by a foreign power as opposed to a mere prank or industrial espionage.

Then officials and legislators need to decide what constitutes an act of justifiable self-defense during and after such an attack.

The first step to improving cyberdefense would be to determine what does, in fact, constitute a cyberattack by a foreign power as opposed to a mere prank or industrial

espionage.

To date, there have been few attempts to create such global norms. In 2013, a group of experts on digital law convened in Tallinn, Estonia, and wrote the Tallinn Manual, the closest thing to digital Geneva Conventions the world currently has. (In 2017, it was updated to the Tallinn Manual 2.0.) It defined the characteristics of a cyberattack, including targeting and disabling critical infrastructure, hitting health care facilities, destroying transportation corridors or vehicles containing people, and attempts to penetrate the computer networks of opposing military forces. The original manual was less clear about disinformation campaigns and hacking elections but did deem interference in a foreign country's elections a violation of state sovereignty if it included an attempt at regime change.

In the run-up to the 2017 German parliamentary elections, a string of cyberattacks led to fears of Russian meddling, but according to the Charter of the United Nations, unless armed force has been brought to bear within the borders of a country, no internationally recognized act of aggression has occurred. This definition of war is hopelessly out of date.

Similarly, cyberattacks in the Netherlands in 2017 and 2018 resulted in the denial of government funding and vital services to citizens, but because conventional battlefield weapons weren't used, the U.N. Charter's provisions weren't violated. Countries are beginning to coalesce around the idea that some forms of active countermeasures are justified in self-

defense, if not in actual reciprocation, under international law.

Reaching an international consensus on what triggers a country's right to self-defense in cyberspace requires a coherent, common understanding on where to draw the line between nefarious economic or intelligence activities and true cyberattacks.

One model could take shape if Russian interference in foreign elections is proved beyond any reasonable doubt. Drawing a chain of evidence between Russian state-sponsored election meddling via a cyberattack and actual election outcomes could lead to a global consensus on what constitutes extralegal military activity in cyberspace. It's already clear that elections in multiple countries have been meddled with, and no militaries have visibly responded. In the U.S. case, former President Barack Obama responded by declaring a month before he left office that the United States would respond at a time and place of its choosing. But his successor has not visibly followed through on that threat, at least in cyberspace.

No definition of a cyber-related war crime can be effective without international legitimacy. If a group of experts actually did convene to create binding digital Geneva Conventions, it's unclear from what source it would derive its authority. NATO sponsored the Tallinn conference, but the Tallinn Manual is nonbinding and was not an official NATO publication. Moreover, the alliance itself is currently on shaky ground, and there's no guarantee that the United States would abide by

any agreement.

In the absence of a binding global accord, the world will remain vulnerable to a motley mix of hackers, warriors, intelligence operatives, criminals, and angry teenagers—none of whom can be distinguished from behind three proxy servers.

In the absence of a binding global accord, the world will remain vulnerable to a motley mix of hackers, warriors, intelligence operatives, criminals, and angry teenagers—none of whom can be distinguished from behind three proxy servers.

It would be nearly impossible to identify perpetrators with 100 percent confidence if they take even rudimentary steps to cover their digital tracks after cyberattacks.

In the absence of a binding global accord, the world will remain vulnerable to a motley mix of hackers, warriors, intelligence operatives, criminals, and angry teenagers—none of whom can be distinguished from behind three proxy servers.

Were disaster to strike Southern California tomorrow, scientific tests and forensic analysis would allow us to tell whether it was an earthquake or a bomb—even if both events could destroy approximately the same amount of property. Yet it would be very easy to confuse a distributed denial of service attack on a U.S. government website launched for fun by a few juvenile hackers in St. Petersburg with an attack launched

by the Russian military to deliberately deny U.S. citizens the ability to register to vote or collect entitlements. Cyber-enabled disinformation campaigns are equally problematic to attribute and to punish. Despite the consensus among experts and intelligence services that Russia tampered with the 2016 U.S. presidential election, it is proving extremely difficult to gain nonpartisan consensus that Russian-targeted advertising purchases on social media constitute hostile acts by a foreign power.

The challenge today is the rapid speed at which cyberspace morphs and evolves. It is changing faster than international summits can be convened, making obsolete any deal that takes longer than a week or two to negotiate. Even if one country can come to an internal agreement on what constitutes a cyberattack from one private party to another, there's no guarantee that two countries could do the same. But they will have to try.

Habits tend to become tradition. That's how the 1648 Peace of Westphalia, intellectually inspired by Hugo Grotius, came to define the modern nation-state and govern international relations. Grotius, a Dutch lawyer and the father of just-war theory, defined the first series of rules by which an anarchic international order could begin to structure itself. After 370 years, the concept of the modern state seems largely set in stone and has been repeatedly reinforced by its use as a framework for relations.

The international community needs new habits for a new era. Leaders must follow NATO's tentative footsteps in Tallinn and convene digital Geneva Conventions that produce a few deep, well-enforced rules surrounding the conduct of war in cyberspace. Cyberwar is the continuation of kinetic war by plausibly deniable means. Without a global consensus on what constitutes cyberwar, the world will be left in an anarchic state governed by contradictory laws and norms and vulnerable to the possibility of a devastating war launched by a few anonymous keystrokes.

This article originally appeared in the Fall 2018 issue of Foreign Policy*magazine.*