HUMANITARIAN LAW & POLICY

Industrial cyber attacks: a humanitarian crisis in the making

December 3, 2019, Analysis / Cyber / Human Costs of Cyber / Law and Conflict / New Technologies

10 mins read

Sergio Caltagirone Dragos

Industrial control systems manage almost every aspect of daily life, from water supply to electricity or industrial production. The number of cyber attacks on these systems is increasing, as is the number of adversaries now investing in such attacks. For societies across the globe, the situation has potentially dire effects: cities could be cut off from water or electricity and economies could be severely compromised. Decisive actions are needed to increase system defensibility and to manage the behaviors of attackers threatening them.

Experts recognize the recent deterioration of the cyber threat landscape. We cannot predict the future, but without a substantial worldwide change in the defensibility of industrial control systems, the following effects are reasonable to expect within a decade:

- Cyber attacks on industrial systems will become ‘commoditized’ and deployable by malicious actors on a whim, disrupting vital infrastructure anywhere for political, criminal, or personal gain.
- Cyber attacks on industrial systems will cause the unexpected loss of primary critical systems, such as medical equipment, levees and dams, drinking water distribution and sewage management, and electric power.
- Cyber attacks on industrial systems will cause significant suffering among populations and damage to economies in regional or national areas, necessitating the mobilization of resources to prevent humanitarian crises.

In this post, I do not describe the cyber threat landscape of today. Instead, I present several interconnected reasons for which we may expect important humanitarian consequences from cyber operations over the next decade.

Increasing vulnerability

The industrial sector, like most sectors, benefits from increased digitalization and network connectivity. Engineers design current and future generation industrial control systems and medical devices with digital transformation in mind. Ideas far away some years ago, such as cloud and internet-connected production systems or medical devices, are now at the fingertips of virtually all industrial equipment operators. However, this connectivity increases complexity and injects new pathways into critical equipment. The more industrial systems rely on digital systems, and the more connected they are to the internet, the greater the risk of cyber attacks against them.

Increasing offensive investment

The list of public attacks affecting civilian industrial control systems and the tools designed to facilitate such attacks is growing, albeit slowly: *a dam* in the United States in 2013, a *steel mill* in Germany in 2014, an *electric grid* in Ukraine in 2016, the *National Health Service* in the United Kingdom in 2017, and *safety instrumented systems* in Saudi Arabia in 2017. This year alone we have witnessed attacks on a *major electricity supplier* in South Africa and a *nuclear facility* in India. Industrial loss from the NotPetya and Wannacry malware measure in the multiple *billions of dollars* by companies like *Maersk* and *Merck*. However, incident response teams uncover dozens of *non-public industrial attacks* per year, if not more, rendering the situation far worse than actually reported.

The knowledge required to attack these systems remains relatively esoteric; many industrial environments continue to be relatively disconnected from the internet. As with all systems, however, knowledge on how to attack industrial systems through cyberspace will increase, and the systems will become more interconnected. More publicized attacks will pressure actors to maintain power parity, and those already active will continue or increase their attacks. All in all, this may lead to a dramatic growth in threats to critical industrial environments in the coming decades.

Increasing proliferation and commoditization of knowledge and tools

There is a real risk that adversaries commoditize disruptive cyber attacks against medical devices and industrial environments. Just as mass communications surveillance was once the bastion of only a few and powerful States, it is now available to rebel organizations, terrorists, abusive partners, and governments. Similarly, the knowledge of how to attack industrial control systems on a large scale will benefit from the increasing digital transformation of these environments. As a result, disruption of drinking water, levees, dams, electric power, medical facilities and devices, sewage operations, transportation, etc., will be at risk of attacks by a variety of actors from every corner of the globe.

Just as with nearly every kinetic weapon system, cyber weapons designed initially by governments to target, disrupt, and destroy industrial control systems risk falling into the hands of unscrupulous and malicious actors actors. Eventually, local warlords may have the capacity to deploy government-grade cyber weapons against a remote target, which would vastly increase their power and influence.

In recent years, private companies have started offering digital tools and services for *surveillance*, *ransomware*, *intellectual property theft*, *location tracking*, and other cyber crime to government and non-governmental clients. In November 2019, malware, spyware, stalkerware and the like were openly advertised with booths and salespeople at *Milipol in Paris*, the largest tradeshow for private industry selling products to militaries, intelligence, and police.

It is likely that criminal private enterprises will eventually enter the market of attacks against industrial control systems, upgrading industrial attacks and coercion through critical infrastructure disruption to a paid service. A future criminal marketing message might offer: “Tell us the water company’s name, and for only $100,000 we will shut down all pumps for one week.”

A growing scale of cyber attacks

This newfound power is unlikely to go unused. For thousands of years, governments, criminals, tyrants, warlords, rebels, and terrorists have coerced and weakened governments and populations by disrupting critical infrastructure such as drinking water (and more recently power) while also preventing the production and distribution of food and medical assistance. Unfortunately, there will be malicious actors in the future, and cyber technology adds another tool to their toolbox.

Due to the interconnectedness of cyberspace, what was once only a local disturbance affecting a neighborhood, a village, a town, or a city will likely grow in scale to affect entire regions and even entire countries. What actors could once do only kinetically – attacking transformers to disrupt power or shutting off individual water pumps – could be done remotely and on a large scale.

Humanitarian crisis

Billions of people rely daily on industrial control systems, the ‘hidden computers’ and networks that underpin modern life. Levies across countries move in tandem instantaneously, preventing flooding, protecting lives and maintaining millions of acres of usable farmland. Manufacturers process food safer and faster, feeding more people and preventing illnesses. Power generation units reliably distribute electricity to large populations, keeping the heating on and economies running. Advanced medical equipment dramatically improves health outcomes and prevents death and suffering.

With increasing connectivity and the proliferation of malware and knowledge, all of this is at risk of cyber attacks. Without these industrial systems, millions or more may suffer from the lack of medical care, food, drinking water, or heating during winter and cooling during summer. It is a humanitarian imperative to protect these systems from disruption and to protect human life.

A beginning, not a conclusion

The international community is standing on a precipice. We have built societies and lives entirely dependent on these systems, yet they are increasingly vulnerable to attacks by those interested and able. It is too late to back away. It's too late to reverse technology. We must confront the challenge.

We cannot let a warlord remotely flood an entire region displacing millions so they can rush in and control the territory. We cannot allow a terrorist to disrupt and disable medical systems from afar. We cannot permit a criminal to disable water pumps during fire season, holding an entire community's property and lives at ransom. We cannot let a State disable electric power during the freezing temperatures of winter to increase their influence in local politics.

The humanitarian crisis and human cost described above is not the world of today, nor is it the world of tomorrow. However, it could be the world ten years from now. Fortunately, this is not a foregone conclusion. Decisive action on different levels of society could avert some of the risk:

- Industrial asset owners and operators must be given greater support to prepare their operational environments for cyber attack, safeguarding services for their customers, and the safety of those working and living in and around these environments.
- States need to work cooperatively to reaffirm existing rules, establish new rules if needed, and find effective ways to monitor and enforce them.
- The technology industry must provide effective and scalable solutions to detect threats against industrial environments at prices that are affordable and usable to clients ranging from a local municipal water authority to the most profitable oil and gas companies.

Importantly, we as a global community must consider the following *position* and the humanitarian imperative confronting us:

"*Any illicit access into civilian industrial control systems (ICS), like electric power, unacceptably places innocent human lives at risk. Decision makers and policy makers worldwide must establish a red line disallowing all forces from operating within civilian industrial networks to ensure civilian safety.*"

The story of cyber attacks against industrial control systems just began, but it's far from over.

Are cyber operations against industrial control systems lawful in time of armed conflict?

Assessment by Kubo Mačák, Legal Adviser, ICRC

Industrial control systems (ICS) supporting essential civilian services, such as medical facilities and devices or civilian power grids, qualify as *civilian objects*. As such, attacks against them are *strictly prohibited* under IHL and may under *certain conditions* even amount to war crimes. In the *ICRC's view*, this prohibition encompasses cyber operations designed to disable ICS or their components even if no physical damage occurs.

Certain types of infrastructure, such as *medical services* or *objects indispensable to the survival of the population*, including the ICS used to manage them, enjoy even more stringent protection under IHL. For instance, drinking water installations, as objects indispensable to the survival of the population, are also protected against cyber operations other than attacks, including those that would render such objects useless.

During armed conflict, an attacker may only launch a cyber operation against an ICS if it constitutes a *military objective*. Depending on the circumstances, that might be the case, for instance, if the targeted system is used for the provision of power and water supply at an enemy military base and if the attack, in the circumstances ruling at the time, offers a definite *military advantage*.

Even then, the attacker must take all feasible *precautions* to avoid or at least minimize incidental civilian harm and *abort the operation* if, for instance, the expected incidental civilian harm exceeds the concrete and direct military advantage anticipated. *Additional restrictions* might apply in the case of water or other specially protected objects.

See also

- Laurent Gisel and Tilman Rodenhauser, *Cyber operations and international humanitarian law: five key points*, November 28, 2019
- Humanitarian Law & Policy Blog, *Human Costs of Cyber – Blog Series*, May-June 2019
- ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflict*, 28 November 2019

Tags: cyber, cyber attacks, cyber security, cyber threat intelligence, Germany, humanitarian, IHL, industrial, industrial control systems, international humanitarian law, international law, Saudi Arabia, South Africa, Ukraine, United States

You may also be interested in: