

Cyber threats in times of conflict

The image of powerful nations releasing their cyber-arsenal to disrupt or cripple their victims' infrastructure, military capabilities or economy during times of conflict has been largely a matter of speculation and Hollywood movies until recently. The war between Russia and Ukraine, the US operation in Venezuela, and US/Israeli attacks on Iran have all offered glimpses into the reality of offensive cyber operations.

Just as with traditional warfare, sophisticated cyber attacks can take years to plan, prepare, and deploy, often sitting undetected until the moment they're triggered. They represent significant investments in time and offensive techniques that have limited shelf lives. Once discovered, defenders will analyze what happened, how to recover, and how to prevent similar attacks in the future.

The Stuxnet blueprint

We got a view of these offensive capabilities in 2010 when stunning stories emerged about a successful US/Israeli operation involving malware that targeted air-gapped Iranian centrifuges used to enrich uranium for their nuclear development program. As reported in IEEE Spectrum, "Stuxnet is regarded as the first cyberweapon that succeeded in destroying industrial infrastructure in an intelligence operation."

Fast forward to the mid-2010s, and Putin's regime started to use its technical abilities to probe for weaknesses and disrupt systems across Ukraine. Andy Greenberg's 2019 book Sandworm documented Russian cyber operations targeting Ukraine including attacks on the Ukrainian power grid in 2015-2016. The implications of cyberwarfare were laid bare as Greenberg describes how NotPetya, a supply chain attack designed to destroy systems, spread beyond the conflict resulting in billions of dollars of collateral damage to companies like Maersk, Merck & FedEx.

Cyberattacks as part of the Russian-Ukrainian war have been relentless for over 4 years now, but defenses have largely held and we haven't seen a knockout blow to either side. Russia continues to use kinetic weapons to target the Ukrainian power infrastructure, punctuating the fact that cyberattacks alone haven't kept them offline.

Ukraine has developed extensive expertise in drones and electronic warfare, with both sides using unmanned systems, electronic jamming and other technologies to locate, disrupt and attack targets. The conflict has become an important laboratory for the integration of digital and physical technologies in modern warfare.

Shortly after the US launched Operation Absolute Resolve January 3rd in Venezuela, reports emerged stating that some impressively coordinated and precise cyber-attacks shut down parts of the Caracas power grid to provide cover for US troops. However as Dr Louise Marie Hurel with the UK think tank RUSI states, "The tactical case for cyber effects in kinetic operations is often overstated." In fact, Cynthia Brumfield reports in CyberScoop that the Venezuelan blackouts may have largely resulted from Kinetic attacks on a crumbling power grid rather than US cyber operations as initially reported.

All of these examples help to illustrate that in a conflict, belligerents will over-state their own capabilities to try to intimidate and demoralize their opponents. This is also true of cyber-conflicts, and the fog of war can make it difficult to tell fact from fiction.

Iran puts cyber retaliation to the test

Immediately following the Feb 28, 2026 attacks by the US and Israel on Iran, there were warnings of substantial Iranian retaliatory attacks by Iran and sympathetic groups. Potential escalation with allies Russia and China coming to Iran's aid was a distinct possibility.

The months that followed have provided a much clearer picture of what Iranian cyber retaliation actually looked like. Rather than a single catastrophic attack capable of changing the course of the conflict, Iranian-linked groups conducted a range of disruptive operations against companies and infrastructure, demonstrating how cyber operations can broaden a conventional conflict beyond the physical battlefield.

One of the most prominent examples was the March 11 cyberattack against US medical technology company Stryker. The company reported a global disruption to its Microsoft environment that affected order processing, manufacturing and shipping. Stryker subsequently said the attack had been contained and that no patient-related services or connected medical products had been affected. An Iran-linked group known as Handala claimed responsibility for the attack.

In late March, Palo Alto Networks' Unit 42 identified activity targeting Rockwell Automation's FactoryTalk software and related operational technology. The US Cybersecurity and Infrastructure Security Agency subsequently warned that Iran-affiliated actors were exploiting internet-facing operational technology, including programmable logic controllers used across US critical-infrastructure sectors.

The broader lesson

What the events of 2026 suggest so far is that cyber conflict is becoming less of a hypothetical "next battlefield" and more of a routine component of modern warfare. The most important attacks may not be spectacular standalone cyberweapons, but persistent operations that complement conventional attacks, disrupt businesses and infrastructure, gather intelligence, create uncertainty and force defenders to spend resources responding.

For organizations assessing cyber risk, this means that the question is not simply whether a country is formally at war. Cyber operations can be used before, during and alongside conventional military action, and their effects can cross borders through multinational companies, cloud infrastructure and global supply chains.

The lesson from both Ukraine and Iran is therefore more nuanced than either the cyberwarfare hype or its dismissal. Cyberattacks have become an integral component of modern conflict, but they have not replaced conventional warfare. In assessing cyber risk, it remains best to prepare for the worst and hope for the best.