ON AUGUST 15, 2011, THE HACKTIVIST GROUP ANTISEC ANNOUNCED it had broken into the personal e-mail account of Richard Garcia, a senior vice president of Vanguard Defense Industries. The group stole nearly 4,713 e-mails and thousands of documents.

On the surface, the incident was similar to the thousands of personal account breaches in cyberspace, except for one factor. Vanguard Defense Industries makes the Shadowhawk unmanned aerial vehicle, which is used not only for intelligence, surveillance, and reconnaissance, but can be weaponized with payloads including grenade launchers, semi-automatic small arms, and signal intelligence units. Information on Shadowhawk may have existed within Mr. Garcia’s stolen e-mail messages. If so, that information could now be in very dangerous hands. What were they trying to achieve?

Theft of intellectual property is troubling, no matter what the victim’s identity. But theft of IP from the defense industry can be terrifying. IP that falls into the wrong hands can have devastating security and espionage repercussions, troublesome competitiveness implications, and can even be used to target employees and families for blackmail or kidnapping.
The worst-case scenario is where theft of IP can change the balance of power and introduce severe vulnerabilities into national defense. If, for example, China were to hack into French or Israeli defense secrets, it might identify vulnerabilities in the target nation’s defenses. Further, once inside, it also might be possible to introduce flaws into defense plans and systems that could go unnoticed for months or even years.

In September 2011, the Japanese-headquartered anti-malware firm Trend Micro identified 32 defense industry computers that had been compromised with remote command-and-control software. Trend Micro reported that eight companies, located in Japan, Israel, India, and the United States, had been victims of a malicious PDF attachment that exploited vulnerabilities in Adobe’s Flash Player and Reader software.

Although cyber-based IP theft is often perpetrated by nation states, attacks on defense industry contractors come from many different actors.

Once the computers were penetrated, the attacking payload then contacted remote command-and-control servers with detailed information about where it had “landed,” and then awaited further instructions. At this point, the attackers not only had the ability to remote-control the victim’s computers, they were also essentially inside the firewall and had the ability to move laterally within each company’s internal network—and had been able to do so for at least four months.

The stolen information could also be used to produce knock-off or fake goods—like medicines, integrated circuits, or even bullet-proof vests—that are then reintroduced into our markets. According to US Attorney General Eric Holder (the nation’s top law enforcement official), “Put simply, when fake goods find their way into our nation’s marketplace, the health and safety of our people can be severely compromised.”

The Trend Micro example makes it clear how virtually all advanced nations (and the defense industry companies that serve them) can become active targets of thieves, terrorists, and other nation states—including those that may also be their allies. Intellectual property theft from defense industry contractors may well have broad-ranging international implications because companies in the defense industry often provide services to multiple nations. Although most defense companies carefully insulate customer organizations servicing one country from customer organizations servicing another country, the IP sold to both countries is often based on similar research. A theft of IP from a multi-national company could have a chain reaction, by introducing vulnerabilities into many nations’ defenses all at once.

Although cyber-based IP theft is often perpetrated by nation states, attacks on defense industry contractors come from many different actors. These include state-sponsored organizations, organizations seeking financial gain (which could range from organized crime to terrorists), activist organizations, and even groups of attackers who don’t have a formal organizational structure, but who utilize “flash mob” methods to summon and incite a large group of participants into carrying out an attack or penetration attempt.
A number of leading US defense contractors detailed the relentless threats they face at the Reuters Aerospace and Defense Summit in September 2011. “Every defense company is constantly under attack,” said Northrop Grumman CEO Wes Bush. “It is a threat that is broad-based. It’s not just from one source…and it’s just unceasing.”

David Hess, president of Pratt & Whitney, added, “It’s not the result of some guy with sneakers in his cubicle hacking away at a computer screen.” BAE Systems President Linda Hudson called the attacks “a very real daily threat to what we do and something we spend a lot of our own money on.”

The losses thus far have been enormous. In a July 2011 speech at the National Defense University, US Deputy Secretary of Defense William Lynn admitted that terabytes of sensitive data have already been extracted by foreign intruders from corporate networks of defense companies over the past decade and that 24,000 files were stolen in a single intrusion in March 2011. “By blunting our edge in military technology, and enabling foreign competitors to copy the fruits of our commercial innovation, it has a deeply corrosive effect over the long-term,” Lynn said.

One approach to defending against the theft of IP is being tested by Boeing. The company is exploring Extensible Access Control Markup Language (XACML) 3.0 and an extension called the Intellectual Property Control (IPC) profile. The purpose of this is to protect intellectual property as it transits between Boeing and its partners.

According to Boeing Information Security Specialist Richard Hill, “What we are getting is a common vocabulary for intellectual property.” Boeing’s Internal Compliance Specialist, Crystal Hayes, continues, “If we are speaking the same language we are better able to control the movement and release of IP.”

If this sounds a lot like a Cold War—one where the spies operate over the internet rather than through notes hidden in magnetized boxes attached to lamp posts—you are not mistaken. Spying and espionage go back thousands of years in human history and will probably continue, in new and interesting forms, for thousands of years into our future. Like governments and warriors throughout history, it’s imperative that our modern governments – and the companies that serve and service them – develop defenses against penetration and practice vigilance to ensure those defenses are used to their best effect.
Intellectual property that falls into the wrong hands can have devastating security and espionage repercussions, troublesome competitiveness implications, and can even be used to target employees and families for blackmail or kidnapping.