AMERICAN FOREIGN POLICY COUNCIL

Information warfare threatens Western corporations

February 6, 2019 **Stephen Blank** *The Hill*

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Intelligence and Counterintelligence; Russia

Since 2014, we have learned just how potent Russian information warfare can be when it targets foreign governments. But as a result, we have tended to overlook the no less disruptive proliferation of attacks against Western corporations. The devastating Chinese hack against the Marriott Hotel chain, the Iranian attack on Aramco in 2015, and North Korea's 2014 attack on Sony are all good reminders. These are hardly the only examples. And as the Chertoff Group and the Foundation for Defense of Democracies just reported, the security of private corporate networks in the U.S. (and probably abroad) represent a tempting and highly vulnerable target for actors like Russia, China, North Korea and Iran.

Neither are such attacks confined to major corporate players. Nor do such attacks only take the form of network penetrations. Cyber and informational attacks on these targets can take the form of disinformation campaigns orchestrated, e.g. by Russia, to besmirch the good name of a corporation, undermine its reputation and thus make it difficult if not impossible for it to secure contracts or funding. If the attack is sufficiently successful, the company either loses its market share or has to go out of business. In that case, the field is open for a pro-Moscow or actual Russian entity to replace it. In Russian parlance, this is known as "Reiderstvo," i.e. corporate raiding and it is a hallmark of the Putin system.

Such attacks do not differ much from the takeover of legitimate businesses by organized crime syndicates. And since Russia is run like an organized crime syndicate, we should not be surprised that Moscow employs this tactic at home and abroad.

For example, since 2017 Russian trolls using classic Russian disinformation tactics have stalked several Western owned international cargo carriers accusing them of transferring weapons to terrorists across the Middle East for the CIA. In fact, these carriers not only carry out shipments of non-lethal goods for the U.S. and other governments, they also do so for the UN and are not owned by any government. These well-steeled and long-standing lies have long been a staple of Russian active measures and disinformation that seek to implicate not just the CIA and U.S. government as supporters of terrorism (when in fact Moscow supports the Taliban, Hezbollah and earlier the FARC as well as terrorism in Ukraine) but also to impugn the reputation of these international cargo carriers.

Politically the aim is to implicate Washington and pro-American governments. Beyond discrediting Western governments they seek to undermine the practice of governments (including the UN) using these shippers to bring humanitarian cargoes to distressed or war-torn areas.

But economically such attacks on large or smaller corporations aim to cripple them unless they accede to the wishes of states like Russia or North Korea as in Pyongyang's hacking of Sony in 2014. Let's also remember the cases of hackers attacking corporations until they pay ransom. In this case the attack on these suppliers also evidently aims at depriving them of capital by undermining their market presence and causing them to lose market share that Russian companies could then step in, reap huge profits for itself, and then use legitimate business operations to cover covert and criminal operations involving international cargo shipping for Moscow and its own benefit. In other words, it's the internationalization of Reiderstvo as well as another front in Moscow's war on the West.

We ignore such attacks on the corporate sector at our peril as the Foundation for Defense of Democracies' report suggests. But not only private enterprises need to defend themselves. That defense of vulnerable corporations must involve public-private partnerships and enforceable sanctions on perpetrators to scotch this snake before it can strike again. Otherwise, what we now see will be merely the beginning of a much greater attack on international business and the global economy. But such attacks do not stop there, they also aim at the international political order. Politics and economics are inseparable here. This is why we need public-private cooperation to defend these targets and also deter and/or forestall future attacks. For if we let Russia and other bad actors attack the foundations of our economic power with impunity, we should know they will then move on to attack even bigger targets and do so without any letup.

Stephen Blank, Ph.D., is a senior fellow at the American Foreign Policy Council, focused on the geopolitics and geostrategy of the former Soviet Union, Russia and Eurasia. He is a former professor of Russian National Security Studies and National Security Affairs at the Strategic Studies Institute of the U.S. Army War College. He is also a former MacArthur fellow at the U.S. Army War College.