Companies Have a Crucial Role to Play in National Security

Author Elisabeth Braw

By Elisabeth Braw

How Companies Are Targeted in a Cyberattack

Immediately after the United States killed Iranian general Qasim Soleimani on Jan. 3 this year, the warnings began arriving: Iran would retaliate by attacking US companies. It would not be the first time Iran has attacked a US business: today the private sector is increasingly a target as countries compete for geopolitical power without having to go to war against one another. But companies shouldn't simply consider themselves victims. On the contrary, they have a crucial role to play in national security.

Six years ago, unknown hackers inserted malware into the computer networks of Las Vegas Sands Corp., the world's largest gambling company. It was a sophisticated attack that brought down three quarters of the casino's servers; restoring them cost more than $40 million. US authorities subsequently established that hackers working for the Iranian government had perpetrated the attack. Las Vegas Sands Corp. belongs to Sheldon Adelson, a controversial businessman and ardent supporter of Israel (and subsequently also of President Donald Trump). Four months before the cyberattack, Adelson had publicly proposed that the US should detonate a nuclear bomb on Iran.

History of Private Sector Being Targeted

The attack against Adelson's gambling empire was an early example of how companies are targeted as countries compete for global power. For centuries, civilians and subsequently also businesses have been targeted as tribes, principalities and countries went to war against one another. Such attacks were simply part of the warfare. The Geneva Conventions, passed between 1864 and 1949, subsequently introduced rules protecting civilians. Companies, however, remained targets in armed conflicts. During World War I, for example, Britain's Royal Navy – aided by France and Italy – blockaded all vessels bearing commodities for Germany and its allies. During World War II, "more than 12,000 mines were laid [by the US] in Japan's shipping routes, territorial waters, and ports as part of Operation Starvation. These mines sank or severely damaged 670 Japanese ships and strangled maritime commerce," as Commander Timothy McGeehan and Commander Douglas Wahl (Retired) of the US Navy note in the January 2016 Proceedings of the US Naval Institute. And during World War II, Britain and the US controversially firebombed Dresden, a city with minimal military value, reducing its companies along with its buildings to rubble. Nazi Germany, for its part, forcibly expropriated companies from owners (often Jews) in countries it had occupied.

What is different today is that companies are being attacked even though no war has been declared. Consider the findings in the 2019 Cyber Readiness Report by insurer Hiscox. Last year 61% of businesses in Belgium, France, Germany, the Netherlands, Spain, the United Kingdom and the US reported having been subjected to a cyberattack in the preceding 12 months, up from 45% in the previous year. Troublingly, an even higher percentage (65%) reported having experienced one or more cyberattacks as a result of a weak link in their supply chains. (This is the first time Hiscox included supply chains in its Cyber Readiness Report.) In addition, businesses are increasingly subjected to repeated cyberattacks. "In every one of the 15 sectors tracked in this report, the proportion of firms reporting one or more attacks has risen sharply. Across all seven countries, the most heavily targeted sector was TMT [technology, media and telecom], where 72% of respondents reported one or more attacks, up from 53% a year ago. Government entities came second (71% reporting an attack, up from 55%), followed by financial services (67%, up from 57%)," Hiscox reports.

Britain's 2019 Cyber Security Breaches Survey, in turn, says that 32% of businesses and 22% of charities report having experienced cyber security breaches or attacks in the previous 12 months. Medium-sized and large businesses are the most affected at 60% and 61% respectively. While the number of attacks has decreased, that does not mean that aggression is abating. The UK Department for Digital, Culture, Media and Sport, the publisher of the Cyber Security Breaches Survey, suggests that one possibility "is a change in attacker behaviour, with more attacks being focused on a narrower (though still numerous) range of businesses".

Not all of these cyberattacks are, of course, linked to governments – but many are. The Council on Foreign Relations, a New York think tank, maintains a database of state-linked cyberattacks (including cyberattacks linked to Western governments). In April last year, for example, German pharmaceutical giant Bayer reported having been attacked by Wicked Panda, a Chinese hacker group linked to the Chinese government. According to cybersecurity firm Crowdstrike, the group's tools have been traced to "contractors who count multiple Chinese government agencies as clients, including the Ministry of Public Security. Observed targeting by the Wicked Panda adversary has focused on high-value entities in the engineering,

manufacturing and technology sectors, aligning with the PRC's strategic economic plans." A plant chlorinating Ukraine's water – a critical function – has been targeted by hackers working for Russia. An Iranian hacker group referred to as APT33, Refined Kitten or Holmium has managed to interfere with the operations of target companies such as power plants rather than simply disrupting them as most hackers do.

Other Forms of Aggression Against Businesses

Businesses are subjected to other forms of aggression as well. Last July, the UK-flagged, Swedish-owned freighter *Stena Impero* was seized in the Strait of Hormuz by commandos from Iran's Revolutionary Guard; initially Iran maintained that the freighter had violated international rules but later stated that the seizure was a response to Britain's seizure of an Iranian oil tanker suspected of carrying oil to Syria earlier that month. Following the *Stena Impero*'s seizure, insurance costs spiked.

Executives worry, too, that disinformation campaigns by governments hostile to countries where they are based or have significant operations could harm them. Imagine, for example, a successful disinformation campaign by Country A against Country B, where Company X is based. By spreading false information about the stability of Country B's government, Country A can – for example – fuel a run on Country A's currency, thereby causing significant harm to business including Company X.

Businesses are, in other words, being targeted and harmed by other countries and their proxies not because any country is pursuing vendettas against them specifically. Instead, they are being attacked as a way of weakening the country or countries they represent. The *Stena Impero* was seized not because the government of Iran wished to harm it or its Swedish owner Stena Bulk, but to protest at the seizure of the Iranian freighter by the UK. In addition, the seizure can be seen as a protest against the Trump administration's campaign against Iran and the Joint Comprehensive Plan of Action (JCPOA), better known as the Iran nuclear deal. By seizing the *Stena Impero*, Iran indicated that it could make the Strait of Hormuz unsafe for international commerce if it wished to do so. That would constitute a severe blow against companies dependent on the shipping route, and against a number of countries likewise dependent on the route.

Challenges for Companies Targeted by Foreign Governments

The reality that companies can be – and are being – targeted as proxies poses a challenge, because virtually no business can defend itself against a nation-state. Even though rare ones might conceivably do so, the law bans private actors from engaging in offensive action against another country, a necessary requirement for credible defence. In the area of cyber, for example, a business is allowed to defend itself but is not allowed to strike back against its attacker through cyberattacks of its own. Nor are businesses permitted to conduct preventive attacks against individuals or groups it suspects of planning a cyberattack. Offensive cyber action is the domain of governments, and with good reason: through offensive attacks, businesses could escalate conflicts with a foreign government to the point where their home government would have to step in with military means.

Nevertheless, it is clear that the current arrangement, where governments are solely responsible for national security, is not appropriate for an era in which aggression is not only of a military nature. It is also in everybody's interest that a country – especially a liberal democracy, which is by definition vulnerable to aggression due to the open nature of its society – is able to minimize disruptions to its society. If hostile attacks result in repeated and extensive disruption, it will not only harm current business activities in that country, and the public along with it. It will also harm the country's standing as a safe place to conduct business. Businesses, in other words, have a role to play in national security.

Expected Role of Business in National Security

It may seem like a novel concept. Indeed, it is. Businesses played a role in national security in previous wars, including World War II, and defence contractors by definition still do so. Today, however, companies of all kinds can play a role in national security. Indeed, Western governments are too small to span a protective umbrella over the entirety of their civil societies – and their doing so would be neither affordable nor desirable for their societies.

But which role should businesses play? During the Cold War, the Nordic countries developed so-called "Total Defence" models that can provide lessons today, even though the threats during the Cold War were rather different from those affecting liberal democracies today. Total Defence was created by Sweden during World War II, when it was neutral and was faced with the overwhelming force of Nazi Germany. Sweden further developed its Total Defence during the Cold War, and Denmark, Norway and Finland too developed Total Defence.

As part of Total Defence, the Swedish government maintained close contact with companies considered of vital importance – including the Stockholm Stock Exchange, the postal service, the

telephone company and the railway company, but also Volvo and Saab – so that the country could keep functioning in a crisis. These companies, known as K Companies, were obliged to keep operations going during a crisis, and key staff were exempted from military service to guarantee that continuity of operations. In some cases, such as with Volvo, Saab and arms manufacturer Bofors, the government subsidized the construction of manufacturing facilities inside mountains, which would protect the companies' production against enemy attacks. Sweden largely dismantled Total Defence during the early 2000s, but is now rebuilding the system, albeit not to its Cold War size.

As part of its Total Defence model Finland has, in turn, perfected the National Defence Course introduced by Sweden in the 1950s. The course, an invitation-only three-week residential course (with subsequent refresher courses) in national security for emerging leaders in politics, business, civil society and the armed forces, is highly sought-after. One of its outcomes is that the Finnish business elite are well-informed about national security and take it into account in their activities.

During the Cold War it was, of course, helpful that many of the companies were government monopolies and thus at liberty to adjust their operations to the government's needs. As the involvement of Volvo, Saab and Bofors show, however, it was possible to get privately owned businesses competing on the global market to play a role in the country's security. To be sure, the Swedish government was able to appeal to the executives' sense of patriotism; at that time, all major Swedish companies were led by Swedish citizens, just as most major companies in other countries were led by nationals of the respective country, and the companies were not owned by an even larger foreign entity.

That is different today. In many countries, leading companies may be ultimately owned by a foreign entity; Volvo is, for example, owned by the Chinese automotive giant Geely. Indeed, even if a CEO feels that he or she has a responsibility to contribute to the security of the country in which his or her company is headquartered, such steps may not sit well with the foreign-based owner of the company. Furthermore, businesses worldwide are now led by the MBA generation, which excels at management and financial matters but has little understanding of national security. Some new market giants even take apparent delight in being as remote as possible from the governments of their home countries: consider Facebook's refusal to provide the US Congress and government with anything more than minimal information about the company's contacts with Russia during the 2016 election campaign.

At the same time, it is in businesses' interest to help keep the countries in which they operate as free as possible from disruptions to everyday life, and free from disinformation that can harm investor confidence in the country and thus the country's economic performance. Finland's National Defence Course would be a good starting point for other liberal democracies. The course provides an ideal vehicle for the government to teach emerging leaders (including, crucially, business leaders) about the foundations of the country's national security and the threats facing it, and the refresher courses allow the government to provide information about new and emerging national security challenges. Furthermore, the course builds a network of rising leaders, who are likely to interact and consult with one another throughout their careers.

Government & Private Sector Collaboration for National Security

Governments of liberal democracies would also do well to regularly invite chief executives, especially of companies in strategic sectors such as telecoms, transportation, electricity, food and waste, to regular consultations, providing them with updates on emerging threats and the national security situation more generally. If those invited were given security clearance, such briefings could include classified information. The provision of regular national security updates by the government would allow business leaders to consider their operating environment in a more comprehensive context than what they are able to read in newspapers and reports from risk consultancies.

That does, of course, not automatically mean that they will alter their decision-making in a way that benefits national security. It does, however, mean that they have a better understanding of national security when making corporate decisions. One should bear in mind that in most liberal democracies, businesses today are not just led by the MBA generation but by a generation that has for the most part had minimal interaction with national security. By contrast, major American firms in the 1960s and 1970s were, for example, often led by men who had served in World War II, and almost all Nordic business leaders had performed military service.

Another step that ought to be considered is incentivizing companies in strategic sectors to play specific roles in support of national security, for example to develop comprehensive contingency plans. Today services that were mostly government-owned until the end of the Cold War (primarily telecoms, airlines, water, electricity and railways) have for the most part been privatised. In most sectors, a number of smaller companies now operate side by side, often as competitors. Companies agreeing to take on a role similar to Sweden's Cold War K Companies could receive government subsidies covering the additional expenditures. Alternatively, or

additionally, they could be awarded special government recognition akin to the Royal Warrant label used in monarchies, which would identify them as "best in class".

A chief executive may, of course, still decide that involvement with national security is not a net benefit to the company. Indeed, with large companies operating globally he or she might decide that contributing to the national security of the large Western country where the company has its headquarters could harm its access to other markets. This freedom of business leaders to make decisions based solely on how they will benefit their company, not the country in question, is one of the weaknesses of liberal democracies. By contrast, in authoritarian countries such as China the government can command even officially private companies to perform specific activities or work in close collaboration with the government.

Legislation could solve this problem. It is, however, a blunt tool, and once a new law is in place, those affected by it tend to respond by only meeting the minimum requirements. A mix of limited legislation and engagement with business leaders, by means of consultation and national-security training, could therefore be the most productive way forward. It would build on business leaders' desire for their companies to operate in stable environments and include government consultations to help inform their decision-making in a way that would benefit the country and by extension their companies. Because government should not favor one company over another, it would be important for the consultations to be open to chief executives of all major players within each strategic sector, the only requirement being that they should have security clearance.

Corporate Ownership Laws Could Play Significant Role

One additional aspect is of great significance: corporate ownership laws. Because even major companies are today not often independent but owned by even larger foreign entities, and because that restricts their executives' freedom of action in the area of national security, liberal democracies should consider their rules for foreign ownership. Although most liberal democracies have legislation restricting foreign ownership of strategic companies, those rules are mostly limited to defence contractors and are remarkably permissive. In the UK, for example, between 2002 and 2018, the government only intervened in eight business transactions on national security grounds. There is, however, movement towards more restriction. In 2018 the US imposed stricter rules through the Foreign Investment Risk Review Modernization Act (FIRRMA). The same year, Germany lowered the ownership stake at which foreign investments in strategic companies require government approval, from 25% to 10%. Also in 2018, the UK government presented a white paper which proposes government approval for acquisitions of over 25% in business selling "strategic goods". The UK government estimates that such rules would lead to some 200 applications for approval each year.

Although similar developments are underway in other liberal democracies, the question is whether such tighter rules go far enough. Should there be an outright ban on foreign ownership of companies in strategic sectors, or would that harm the vibrancy of the global market on which companies in Western countries depend? It is worth remembering that China imposes severe restrictions on any kind of foreign companies operating in the country.

Conclusion

The prosperity of liberal democracies from Japan to Canada depends on the success of the market. Despite the messiness of a free and open society, during the Cold War the US outshone its rival, the Soviet Union, measured by standard of living. In 1989, the GDP per capita in the Russian republic within the Soviet Union was $3,428 (measured in current US dollars), compared to $22,857 in the US. Japan, no stranger to geopolitical aggression, performed better still, with a GPD per capita of $24,813.

The challenge, as has been outlined in this article, is that today's national security threats can – and do – directly harm companies. Not every proposal put forward in this article can be adopted by every liberal democracy. Each government can and should, however, urgently consider how it can involve its private sector in national security – whether simply by information-sharing or by also incentivizing companies to play an active role in minimizing disruptions to the country in case of a cyberattack or indeed another type of attack.

The former, of course, informs the latter: business leaders of companies in strategic sectors who properly understand national security challenges are more likely to be willing to commit their company to national security-related moves that an executive focusing solely on the next quarterly report would dismiss as a distraction. The equation boils down to one fundamental reality: because businesses today are targets of geopolitical aggression in a way they have not been in the past, it is unquestionably in their interest to do their part. They just have to be given the opportunity to do so, and the framework for collaboration with the government. JS

Elisabeth Braw is a senior research fellow at the Royal United Services Institute in London, where she leads the Modern Deterrence Project.