GUY CARPENTER

Global Cyber Terrorism Incidents on the Rise

The nature of the terrorism threat facing society has changed considerably in the last 20 years. Previously, governments and (re)insurers structured their mitigation strategies and responses to deal with attacks that were large in scale.

Recently, though, we have seen a spate of smaller, less sophisticated, yet no less appalling acts of terrorism across geographies that involve mass casualties and fear-inducing events. And the type of threat will continue to change as new technologies and opportunities reveal themselves to terrorist organizations – cyber terrorism is an example of a newly developing frontier within the peril.

Guy Carpenter has produced a new report, "*Terrorism: A Maturing Market Meets an Evolving and Expanding Peril,*" which focuses on the changing and evolving nature of terror attacks around the world and the (re)insurance industry's innovations and solutions developed to meet the changing needs. Here, we present the themes around the cyber peril discussed in the report.

Traditionally, most cyber-attacks have been carried out by criminal organizations, with the majority of incidents failing to register on an enterprise risk scale of businesses that faced significant setbacks. In 2017, this dynamic changed with the WannaCry and NotPetya incidents. These two attacks affected organizations in more than 150 countries, prompted business interruption and other losses estimated at well over USD 300 million by some companies, brought reputational damage, and resulted in loss of customer data.

In December 2017, the U.S. government took a rare step and attributed the WannaCry attack to hackers backed by North Korea. WannaCry and NotPetya exposed a systemic risk and affected a broad cross-section of businesses without specific targeting, demonstrating the potential for escalation in the threat of cyber terrorism.

1. The landscape for points of attack is growing. Traditional physical processes carried out by industrial control systems — including critical infrastructure industries such as power utilities, water treatment services, and health and emergency systems — are coming online. Guy Carpenter affiliate Oliver Wyman forecasts that 30 billion connected devices will be in use by 2030, creating more assets susceptible to attack and adding more vulnerabilities to be exploited.
2. Cyber threats are becoming more advanced. The upsurge of highly skilled hackers, often nation-state supported, is coinciding with the development of more sophisticated tools that are likely seeping into the broader environment through a thriving black market.
3. The consequences are high. Companies are now deeply dependent on their systems and data, and interference with those assets can materially affect market capitalization and endanger executive leadership, reputations, sales and profits. Failures in cybersecurity have the potential to destabilize an enterprise overnight.
4. A shift has begun to take place in the nature of cyber incidents; from affecting primarily consumers to having an impact on global political or economic systems as a whole. Examples of this changing trend are the recent headlines covering the banking industry. Large scale cyber-attacks on the banking industry can result in stolen money and personal information entrusted by consumers to these institutions and also, in a worst-case scenario, cause a "run" on the global banking system.

Terrorist groups have ambitious goals for cyber-induced attacks. The industrial control systems that support the electricity industry were largely sealed off from external threats. However, the protections that came with the isolation have weakened with the introduction of automated controls managed through interconnected network systems. As automation grows, so does the opportunity to manipulate an industrial control system through a cyber-attack.

For utilities and other infrastructure facilities, the potential costs of a power grid interruption as a result of a cyber-attack can include:

- Lost revenue;
- Additional expenses to restore operations and to improve cybersecurity defenses;
- Regulatory fines and additional scrutiny; and
- Reputational damage.

Such attacks, though rarely made public, are occurring more frequently. As can be seen in the figure below, the potential perpetrators of acts of cyber terrorism can be separated into five categories.

Although the motivations, capabilities and priorities vary among the groups, each can wreak havoc on a global scale; with ever-increasing funding, these attacks can become more catastrophic.

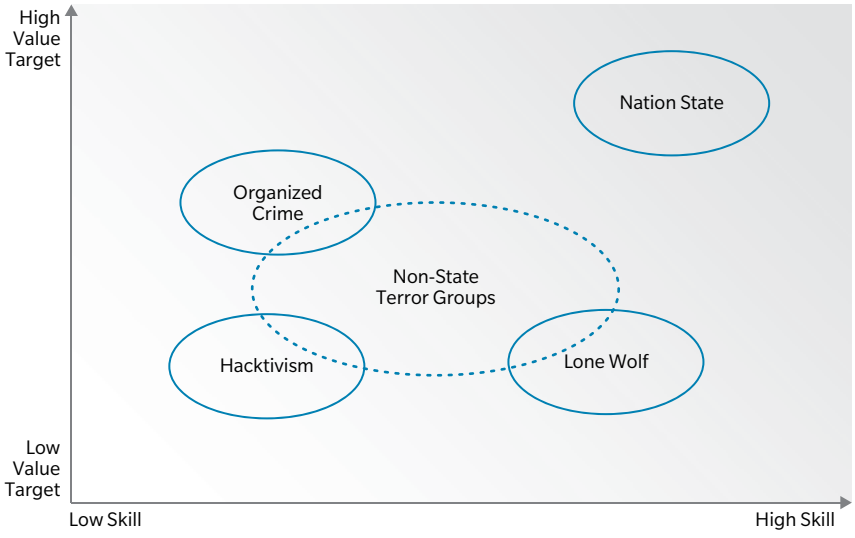
As these factors converge, opportunity could combine with existing motives to inflict catastrophic cyber terrorism losses for businesses. Over time, cyber insurance policies have evolved to cover the failure of technology and the resulting interruption or loss of revenue. Insurers are also increasingly recognizing the interdependence of businesses, especially through technology. Many cyber policies now contain provisions for business interruption and contingent business interruption, including those involving disruption of an organization's supply chain from a data breach.

Business interruption coverage has become a more common coverage component within cyber insurance policies over the last 24 months. Reinsurance solutions in the cyberspace tend to follow the security and privacy coverage offered in the insurance market. Although reinsurance contract wording varies, cyber insurance typically covers network security incidents regardless of the political or ideological beliefs of a non-state actor.

Guy Carpenter's dedicated Cyber Solutions Specialty Practice and Global Cyber Center of Excellence work with professionals around the world to provide risk transfer solutions to help companies quantify potentially catastrophic scenarios and identify the right way to manage, spread and transfer the associated risks. We structure a broad range of tailored reinsurance solutions utilizing our in-house modeling capabilities combined with our investment in third-party models to create our own best-in-class, holistic view of cyber risk for our clients.

The potential perpetrators of acts of cyber terrorism can be separated into five categories: Organized Crime, Hacktivism, Non-State Terror Groups, Lone Wolf and Nation State.

Quadrant threat intelligence model of cyber capabilities



Source: Pool Re