Cyberattacks: Creeping Threat Must Be Prioritised and Tackled

By Lord Waverley

The scale and complexity of cyberthreats being faced internationally underlines the case to bring added awareness on this crucial issue

Cyberactivity, in this world of obfuscation, is a worldwide phenomenon and affects us all. The entire social infrastructure of how we communicate and live our lives has altered permanently, and so the need for mechanisms to monitor, detect, protect against and repel incursions constitutes challenges faced by all cyber experts globally. Cyber is the driving force of our existence today and has transformed the world in which we live; from the way that we shop and the medical care that we receive to the use of capabilities in battlespace operations in military warfare, cybercrime, state-sponsored hacktivism of foreign critical national infrastructure and ransomware attacks on digital currency. Cyber confrontations have transformed 21st Century societies. T

he responsibility of government is to provide the first line of security and last line of defence, from the use of capabilities in battlespace operations during military warfare to cybercrime, state-actor interference in other sovereign states' critical national infrastructure and governance silos to the much-vaunted cyber interventions in national electoral processes. Cybersecurity is a huge problem, and the global response is not moving at the necessary speed. "Plan for the worst" should be the mantra. A major challenge is that it is hard to investigate given an occasional lack of intelligence-sharing between agencies, the inconsistency of the approach of Interpol and the lack of direct communication between banks.

All this compounds the problem. Threat intelligence, for example, should not be beholden to the vagaries of political impasse. There are too many gaps and inconsistencies between the way that different agencies collect, process and use evidence. Scrutiny of the required outputs, matched against clearly defined intent, is essential to gain understanding of the required operating framework and ensure the supporting capacity is sufficient. An isolationist, compliance-based approach to regulation, for example, will lose the race against cyberthreats. The task is so immense that government alone does not have the resources to face up to this issue.

The solution lies in partnership – essential partnership between public and private sectors, and between states and agencies. A keyword throughout should be "awareness"; government should work to ensure businesses are aware of the manifold initiatives and their contribution to them, and convince them of the need to view cybersecurity skills within businesses as a priority. Lack of skilled workers makes this harder. It is essential to agree cross border rules of the game and the legal framework to enshrine them.

Cybercrime networks are international and have merged with organised crime covering terrorism, human trafficking, drug trafficking and child abuse. Within the military space, cyber doctrine does not include a sufficiently common approach, including the underpinning doctrine that informs and directs supporting and enabling activities. It is perceived that an interoperable capability gap exists, and in adversarial activity we are outmatched, outnumbered, and – more importantly – doctrinally outmanoeuvred. Another challenge is that companies often resist investing fully in their IT infrastructure and cybersecurity, believing it cheaper to clean up a mess than to prevent it in the first place. Reputational and financial damage is too often caused by not taking these threats seriously.

The poor handling of breaches may also reveal deeper corporate failings. Mandatory reporting of cyber breaches has begun in some countries, but more must be done to raise awareness of the global nature of the threats. Threats will grow in volume and severity as criminal gangs gain access to more sophisticated tools and become reckless in using them. Emphasis should also be placed on internet and related higher education. The opening of cyber schools, as centres for advanced cybersecurity education, should offer a variety of hands on programmes tailored for a wide range of people with different levels of cybersecurity qualifications and skills, from school and university students to cybersecurity experts. Those who will lead in fundamental and applied research into quantum physics, quantum cryptography and quantum blockchain development will develop an edge.

The importance of the development of secure communications infrastructure in development of quantum is the route forward and presents opportunities for government and the private sector to benefit from secure conferencing and secure data-transfer. Although quantum computers are still in their infancy, it is estimated that once fully developed they will be able to crack current public key encryption infrastructure within 15 years. So, the race is on to develop hybrid solutions to protect current and future data from the power of those quantum computers. Failure will rest with the international community if it does not come together with a collective approach to pass regulation and standards in the form of an international treaty or agreement.

On the international front, while Russia's capabilities and techniques are well-documented, it is China that is fast assuming the mantle of world leader in cyber development. President Xi has outlined plans to turn China into a cyber superpower. Through domestic regulations, technological innovation and foreign policy, China aims to build an impregnable cyber defence system and, increasingly, a separate government-controlled internet. State-led efforts in that country are central to this, with a focus on artificial intelligence, quantum computing and robotics, among other technologies.

The Cyberspace Administration of China has responsibility for controlling online content, bolstering cybersecurity and developing its digital economy. Its investment in research and development now stands at 17% of global R&D spend. China has created an interlocking framework of laws, regulations and standards to increase cybersecurity and safeguard data in governmental and private systems, with surveillance a key feature, aided by facial- and voice-recognition software and artificial intelligence. It has required companies – this has become a trend – to store data within China, where the Government will have few obstacles to accessing it. So what should be done, and by whom, to rein in cyberthreats? It is high time to have a serious discussion about the international legal framework in which cyberwars take place. Yet the last UN discussions by a group of experts took place in 2017, with no consensus reached.

The UN, however, is the best forum to deal with this. Fundamental and innovative approaches are required, and it would be helpful to define such fundamentals as what constitutes a cyberattack, who should decide on the response, and what role should the private sector play in assisting governments.

I venture 16 specific initiatives:

1. Support a call for a global move to outcomes based regulation and legislation, as opposed to the mandating of standards;

2. Form a regulatory framework that forces dialogue between friends and foes alike;

3. Implement initiatives to limit inappropriate meddling that sows discord, either domestically or from abroad;

4. Enable enhanced co-operation within the public sector and continuous dialogue with the private sector;

5. Recognise that the private sector will play a central role in future international cyber governance;

6. Encourage financial services to take a peer-to peer approach to tackling cybercrime, starting with greater dialogue between major banks;

7. Place maximum endeavour in technical co ordination and information sharing;

8. Establish a mechanism whereby financial services institutions are enabled to share information and intelligence, and work together more quickly and effectively;

9. Encourage further development of the cyber insurance industry to bridge the gap between the identification of liability and the lack of data consistency;

10. Define a universal definition of “cybercrime”, “cyberattack” and “cyber threat”;

11. Promote governments coming together through the United Nations to take an approach that treats cybersecurity in a sphere of its own;

12. Strengthen incident response functions of the appropriate agencies and, in doing so, provide clearer guidance on what a reportable incident is;

13. Promote advances in the practical application of quantum physics to achieve secure communications channels;

14. Establish cyber schools for advanced cybersecurity education;

15. Encourage international cybersecurity information-sharing partnerships and further support sector-specific information-sharing centres;

16. Finally, but possibly most importantly, promote global discourse.

I end where I began. The strategic direction of where we go and where we want to be is essential. The scale and complexity continue however, and it is essential to be diligent in our addressing this fundamental issue of our time.