CYBER SECURITY

The internet was initially designed to be an open and democratic environment for information exchange. However, the increased use of this venue to perpetrate deviant actions, including crime and terrorism, and the never-ending interplay between technology and society's daily activities made the calling for "security" a powerful argument to justify the downplay of liberties on the internet. While states are trying to protect information systems, especially critical infrastructures, and data (and therefore themselves and their population), civil society, especially minorities and activists, are trying to make their voices heard through digital platforms.

Each of these three actors – states, civil society, companies – tries to push the security discourse in one way or another to either augment surveillance or the control of information flow or diminish it. Governance, disinformation, and criminality are active topics involving this delicate balancing between liberties and security in cyberspace. Similarly, there are human rights, mainly privacy and freedom of speech, and economic advantages and disadvantages.
Initiatives have been started both by states, e.g., the Paris Call (2018), and companies, e.g., the Digital Geneva Convention (2017), the Charter of Trust (2018) or the Cyber Security Tech Accord (2018). In 2019, the Global Commission on the Stability of Cyberspace (GCSC) published a final report on advancing cyber stability that touched upon this theme and stated: Stability in cyberspace means everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner. Thus, cyber stability must be linked not only to multi-stakeholder engagement and decision making but also to the building of trust. Indeed, according to Ischinger (2019:165), "trust is the cornerstone of cyber diplomacy, as it is diplomacy in general. Without mutual trust, binding norms cannot develop, much less succeed".

Most of the challenges for cyber security are also challenges for privacy and data protection. Cyber security is by no means a static issue with a permanent solution. Threats to information in cyberspace evolve quickly and, more recently, have expanded into new channels such as social media and mobile technologies. As organizations strive to keep pace with the changing landscape created by innovative technologies, social practices and ever-changing threats, data produced, collected and collated on a massive scale can be left vulnerable to those cyber threats. The following are some of the emerging challenges for data protection and cyber security.

Complexity of the Connected Environment

The continuing evolution of cyberspace, as a fully electronic world created by interconnected networks in parallel with our physical environment, is characterized by an enormous amount of data. The modern economy increasingly depends on vast quantities of digital data that are generated through financial transactions, communications, entertainment, travel, shopping, online browsing, and hundreds of other routine activities. Data elements are continually being combined, connected, compared and linked to other information as organizations try to capitalize on its value and to offer new and improved services to their users. The electronic systems and digital networks that facilitate these transactions and communications also capture people's preferences and other personal details, and track their

online and, increasingly, physical movements. The volume of data generated in cyberspace can only increase exponentially once the "Internet of things" becomes a reality, and sensors within devices autonomously report on location, status, surrounding environment, provide real-time updates or help monitor and control devices remotely. Threats in cyberspace will continue to target the weakest links in any complex web of business relationships or government processes, meaning stakeholders in cyber security efforts have a shared role in protecting the infrastructure and the information that flows through it.

Growing Sophistication of the Threat

The interconnected systems in the cyberspace that are globally accessible are inherently vulnerable. As the scale of information flowing through cyberspace has expanded, so too has its value to corporations, government, and those with malicious intent. The data trails of citizens now leave a larger footprint across cyberspace , leaving them more exposed to threats. Wherever there is an opportunity to profit there is usually a market for criminal activity, but as Gabriella Coleman notes, there has also been a "professionalization" of hacking and cyber-crime, making these activities much more sophisticated. State- sponsored threats, conducted or condoned by a nation state, are also becoming increasingly common. These are sometimes referred to as Advanced Persistent Threats (APTs) and are usually well educated, well-resourced adversaries who focus on the theft of secrets including intellectual property.

Threats are Moving to the Mobile Sphere

In the next three years, the number of cell phones in use will exceed the global population. The mobile devices can contain a goldmine of personal information. People routinely carry their mobile devices everywhere and use them for almost anything imaginable; people communicate with friends, access email, take photos and video and upload it to the web, play games, track distances, locate nearby stores and restaurants, find directions to specific locations, access their bank accounts, surf the web, monitor their health/physical activity, keep track of appointments or log to-do lists. Organizations are all striving to reach consumers and clients on the devices they use every day, but alongside all of these conveniences for the consumer is the possibility for new vulnerabilities or opportunities for cyber threats.

A recent study notes that one of the significant concerns facing the mobile industry is how to address the skyrocketing amount of malware on mobile devices. Malware can easily be distributed to mobile devices through malicious apps within smartphone app stores which appear safe. Furthermore, the use of free public Wi-Fi can also put mobile devices at increased risk of having data intercepted.

The "Big Data" Paradox: Is it a Bigger Risk or a Solution?

"Big data" can be defined as vast stores of information gathered from both traditional sources and, increasingly, new collection points (e.g. web data, sensor data, text data, time and location data gleaned from social networks). The insights derived through analysis of big data are often touted as the solution to almost any problem or issue. However, this data-driven approach raises two distinct issues from a cyber security perspective: how to secure information in a big data context and the use of new data analytics to sift through network information including personal information, in order to predict security incidents. Security breaches will have a potentially serious impact upon "big data" providers, as the use of big data is fairly new to most organizations and the vulnerabilities and risks may not be well understood. For many, breach preparedness is still not a priority

In recent years, reports of privacy breaches have become increasingly common, with potentially significant consequences for affected individuals. Many of the risks and impacts of cyber incidents are shared between governments and the private sector, but it is most often the private sector that is on the front line in confronting these threats, given that they control the vast majority of the telecommunications infrastructure. Several recent reports have indicated that a large number of businesses are unprepared for, and indifferent to, cyber threats, and lack proper contingency plans.

Compliance Vs. Risk-Management

Organizations are required to comply with various laws and regulations in order to operate in particular jurisdictions or across various jurisdictions. When it comes to security, however, a mechanical approach to compliance does not necessarily mean that the organization is secure. In fact, blindly pursuing compliance may actually put an organization at increased risk specifically because it is focused on a "check-the-box" compliance model leading to a false sense of security, whereas performing proper risk management requires organizations to scour and identify areas where additional safeguards are needed. A risk management approach naturally complements compliance obligations. The challenge for organizations is to understand that security is not simply a matter of meeting minimal compliance standards, but rather, a question of engaging in effective risk management and dynamic implementation of security.