Security Network Munich

EXECUTIVE SUMMARY

MCSC MUNICH CYBER SECURITY CONFERENCE 2020

www.it-security-munich.net

MCSC MUNICH CYBER SECURITY CONFERENCE 2020

Fail safe – Act brave: Building a Secure and Resilient Digital Society

Hotel Bayerischer Hof / Munich, February 13, 2020

EXECUTIVE SUMMARY

The world is racing full throttle into a connected reality with new technologies like artificial intelligence; cloud, edge and quantum computing; and 3D printing. At the same time, the rise of the Internet of Things – connected cars, toys, appliances, homes, medical devices and even wearables – is creating new threat vectors that threaten not only data confidentiality, integrity and accessibility, but also physical safety. 2020 will accelerate a central paradox of cybersecurity: even as technology becomes more sophisticated and deeply integrated into every aspect of daily life, the vectors of cyber vulnerability are getting higher and growing.

Against this background, the 6th annual Munich Cyber Security Conference brought together numerous expert speakers and over 200 high level guests from Europe, North America and Asia at the Bayerischer Hof to discuss tomorrow's cybersecurity challenges. Three overarching themes emerged from these discussions:

Trust remains the connective issue that holds the digital world together. Effective cyber security requires "all-of-society" approaches based on trust and social cohesion. Building that trust requires evolving definitions of what constitutes critical infrastructure. Already the EU, the US, Japan and other democracies are redefining voting systems and the 5G Internet backbone as critical infrastructure. The COVID-19 crisis has drawn into high relief the security importance of medical supply chains, equipment and hospital infrastructure. It also requires movement to risk-based approaches that emphasis deterrence, protection, and resilience from cyber attacks.

Our threat communication must evolve to meet the moment: Society must move from a "need to know" to a "need to share" imperative. This means created denser information sharing communities– from ISACs and ISAOs to new models of confidential social media platforms like those pioneered in Israel, specifically for CISOs to share threats. Hubs like ENISA are bulking up their work to create greater information sharing as well.

Even in the age of digital sovereignty, cyber cooperation must increase across borders and across sectors: Digital sovereignty is becoming an important policy objective in Europe and globally. But this relates to management and control of digital devices. It is not digital autarky. Quite the opposite, mastering cooperation across borders, sectors and device generations will be key to assuring cybersecurity. Incentives must be developed to encourage private sector actors like IoT manufacturers and supply chain vendors to work together to establish and adopt cyber norms and cooperate with others like governments. Regulation will often be too slow to keep pace with technological development. This is why cybersecurity by design is aided by constant cooperation.

Ultimately, cyber security is a question of vigilance. The threats in the digital world – like technology, itself – are not static. Nor are they hemmed in by borders as the 2017 WannaCry attack demonstrated. The urgency to address cybersecurity has never been greater. It is time for a shift to occur from awareness to action.