Twitter Thread by Amy Ertan

Amy Ertan
@AmyErtan

New 2020 cyber trends report now out!

> NEW report by #CCDCOE researchers on 2020 #cyber trends and #lessonslearned they provide for armed forces in order to be better prepared in the future #collaboration #360degreeviewhttps://t.co/VoacrIHxqU pic.twitter.com/mXoflZ5cUe
>
> — NATO CCDCOE (@ccdcoe) January 19, 2021

The new Recent Cyber Events and Possible Implications for Armed Forces report gives high-level analysis on major 2020 cyber trends - direct link to report here: https://t.co/QRAhG3TXIw

Section 1: Overview of Solarwinds and the extended campaign that resulted in the breach of several US government agencies. A discussion on supply chain security management and how vulnerabilities compounded to make the attack possible (and un-detected).

Section 2: A development of cyber norms and international law. The pandemic, state pronouncements and UN-sponsored processes on international law and cyber, space recognised as a domain & the plans for Tallinn 3.0. See CCDCOE's Cyber Law Toolkit for more: https://t.co/5T4ry5wAK4

Section 3: 5G and supply chain infrastructure - the importance of secure communications with implications for both civilian and military use. Noting the use of legislation and market competitors, the @CCDCOE announced a major research project into 5G rollouts in 2021.

Section 4: The Future of AI and Security. AI-enabled is still relatively immature - but has vast potential capabilities. Fake news and applications in cybersecurity are both pressing areas of focus, as are long-term focuses on interoperability and international collaboration.

Big thanks to our CCDCOE Intern @marguer_ite for her excellent contributions on this topic!

Section 5: Ransomware in 2020. COVID-19 themed email campaigns and an attacker focus on healthcare providers. The @CCDCOE will be releasing the 'Cyber Investigator's Handbook' in 2021 - a guide providing the cyber community with guidelines on managing and handling an incident.

Section 6: Attacks on Critical Infrastructure. The pandemic represents 'perfect storm' for CI attacks- remote management of systems, decentralised workforces, expanded outsourcing and outdated software. Vaccine distribution infrastructure a priority moving forward.

Section 7: Digitalisation and the 'Digital Workspace'. NATO and affiliated Agencies have all had to manage the shift to remote working - raising interesting challenges around interoperability and secure platforms to share information. Trial and error helped the CCDCOE adapt.

That's all folks. For a deeper dive into the content - the full report once again: https://t.co/QRAhG3TXIw. The authors are open to feedback and suggestions - contact details at end of the report.