Cyber-Insecurity: Regulating the Future

29 OCTOBER 2024

Tolga Borucu



Imagining a world where air fryers can be used as weapons is not becoming so difficult these days. The notion that everyday devices can be breached by cyberattacks to put users at risk seems to be a nightmare. To establish resilience against this prospect, institutions propagate awareness on topics of cybersecurity. The unexpected dangers emerging from any cybernetic device signifies the importance of a "cyber-conscient" society. Community-wide acknowledgement of security practices and following trends in policy making such as the EU Cyber Resilience Act will diminish the feeling of insecurity posed by potential breaches. The recent cases of faulty software

impacting an unaware individual or entity will help the international consciousness on matters of cyber-resilience and digital vulnerabilities.

A cyber-conscient organism such as a state, institution, or a person would be one avoiding dangers of cyber-attacks and protecting its property or structure through developing measures to undermine disastrous acts. These acts could be moments of such crises where a software can malfunction and cripple an entire industry. A cyber-conscient society would be one that does not allow volatility in security which could end up creating a crisis, it would be safeguarding against evolving cyber threats with regular awareness propagation and stringent security protocols. Furthermore, there are cases when a country-wide improper use of software can end up proving the unpreparedness of an entire state. Recently, the Israel-Palestine conflict in the Middle East exploited civilians in Lebanon through their use of obsolete technology in September 2024. Despite falling behind modern phones, pagers are still used in certain fields, such as medicine. A shut-down of multiple sectors inside a country can happen through exploiting undeveloped infrastructures, as it has been seen by this case at hand. Not being conscious of newer technologies and policies can result in being affected by a potential conflict. Keeping up with the safest technologies, software, and simply following the trends of the market assist us in protecting ourselves from security breaches. To achieve this outcome, it is evident that people should be more aware of the security threats which are presumed to be harmless and keep up with the constantly changing world of cybersecurity.

Individual resilience became globally known after the Lebanese case, but the main discussion for private sector preparedness against moments of crises still continues to be only about intelligence attacks. Searching for solutions such as quantum computers reveals that institutions are exploring new encryption methods to counter the malicious attacks. Nevertheless, the CrowdStrike Incident proved that even an update to a software in daily use can undermine our efficiency. From local municipalities to financial institutions, structures seek help through developing autonomous software after noticing their dependence on the global systems such as Windows. Independence and awareness in cybersecurity is critical, and the CrowdStrike incident enlightened entities from governments to businesses, pushing them to research more local and particular security technologies. In an era of globalisation, our health, economy, and politics is dependent on cybersecurity and this incident made us conscious of that reality by showing the vulnerability of unregulated technology.

At the government level, security depends on the efficiency of protection a state offers to its citizens. Lobbying and policymaking for cybersecurity is a necessity in the modern world due to the constantly changing world of technology. The need to develop structures that contain the fog of unforeseen outcomes is acknowledged by international and national authorities through preparing policies which raise awareness. “EU Cyber Resilience Act” (CRA), which has been adopted by the Council in 10/10/2024, is

one of them and this attempt to curtail insufficient digital infrastructure throughout the European Union signifies the cybersecurity enhancer role of manufacturers and service providers in the sector. Corporate advocacy efforts and highlighting flaws occurring in the private sector by the legislative bodies are complementary to each other, and EU Cyber Resilience Act provides the ground rules for this alliance against misconduct of technology.

The adoption of the CRA signifies the future of technology regulations throughout the globe. Allowing member states to investigate national level products and forcing compliance through cooperation between governments and corporations (Article 43) also imply that states are legitimate in their security concerns for suspecting malicious intent in technological products. Under the act, compliance includes rigorous standards such as audits and mandatory reporting which also promotes transparent legal entities. The EU Artificial Intelligence Act and the expectation throughout the globe for its outcomes also create expectations for the CRA. Supposedly "a Global Regulator", the EU policies result in globally adopted laws and strategies, such in the case of the General Data Protection Regulation. The transnational entity shifts its policies towards the field of cybersecurity, and signals that states are going to put importance to becoming cyber-conscient as much as the security.

In an era defined by advancement and globalisation; cyber vulnerabilities are no longer exposed only through attacks, but through unobserved use too. The Lebanon electronic device attacks and the CrowdStrike outage have revealed the consequences of outdated systems and inadequate practices. Political institutions, corporate entities, and individuals are all open to possible devastation unless there are compliance procedures implementing coordination in public. Similarly, the CRA is a pivotal inspiration for international community members to develop frameworks against emerging threats. Understanding its emphasis on aligning state and corporate work towards sustainable resilience cooperation can lead to efficient policy making and better crisis management for interconnected societies. Maintaining and promoting this coordination throughout the world has become a trend after globalisation in the cases we have mentioned before, and opportunities of cooperation exist for cyber resilience too.