KEY TERMS FROM THE CYBER SECURITY ECONOMICS FOR EMERGING MARKETS

01. **Critical infrastructure:** Systems and assets, whether physical or virtual, that are vital to the nation, and whose incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (NIST, n.d.).
02. **Cyber:** Refers to both information and communications networks (NIST, n.d.). The prefix "cyber" is etymologically rooted in the Greek definition of *kubernetes,* which implies the interface and interaction of the biological and the mechanical (Van Puyvelde and Brantly 2019).
03. **Cyber capability:** A system's potential to maintain the confidentiality, integrity, and availability of computers, networks, and their resident data or data in transit. Cyber capability is a combination of mutually reinforced technical, physical, and procedural controllers and measures (NIST, n.d.; Van Puyvelde and Brantly 2019).
04. **Cyber incident or cyber event:** An event or the end result of any single unauthorized effort taken using an information system (for example, computer technology) or network that resulted in an actual or potentially nationally relevant adverse effect on any of the three layers that constitute cyberspace, including information systems, networks, and/or the information residing therein (Harry and Gallagher 2023; NIST, n.d.).

05. **Cyber incident response:** Response to threats and the mitigation of violations of cybersecurity policies and recommended practices. Incident response allows victims to detect, contain, and recover from security incidents (NIST, n.d.; Taddeo 2019; Woods et al. 2023).

06. **Cyber risk:** "Risk" describes possible negative consequences (harm) weighted by the probability of occurrence, and "cyber" restricts the scope to incidents caused by logical (as opposed to physical) force (Woods and Böhme 2021). The harm could be related to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts on organizational operations (mission, functions, image, or reputation) and assets, individuals, other organizations, and the nation (NIST, n.d.).
07. **Cyber threat:** Any circumstance or event with the potential to have an adverse impact on victims' operations in cyberspace. It is also the potential for a threat source to exploit a particular information system vulnerability successfully (NIST, n.d.).
08. **Cyberattack:** Malicious activity attempting (successfully or not) to gain control of an information system without permission, to disrupt, collect, disable, destroy, degrade, or deny information system infrastructure or the information itself (NIST, n.d.).
09. **Cyberattack surface:** The set of points on the boundary of a cyber system, a cyber system element, or a cyber environment where an attacker can try to enter, cause an effect on, or extract data from that system, system element, or environment (NIST, n.d.).

10. **Cybersecurity:** Systemic security in cyberspace to ensure the availability, integrity, authentication, confidentiality, and nonrepudiation of all components of cyberspace, including systems, information, and data. Instruments for achieving cybersecurity include any technology, measure, or practice that aims at preventing cyber incidents or mitigating their impact (IBM 2023; Van Puyvelde and Brantly 2019).

11. **Cybersecurity awareness:** A learning process that aims to focus attention on security and change individual and organizational attitudes to realize the importance of cybersecurity and the adverse consequences of its failure (NIST, n.d.).
12. **Cybersecurity domains:** At a high level of abstraction, cybersecurity goods and services can be bundled into robustness of digital systems (secured by design systems), resilience of digital systems (sustainable systems), and incident response capabilities (Taddeo 2019).
13. **Cybersecurity resilience:** The ability of an information system to continue to: (1) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (2) recover to an effective operational posture in a timeframe consistent with mission needs (NIST, n.d.).
14. **Cybersecurity robustness:** The ability of cybersecurity measures to operate correctly and reliably across a wide range of operational conditions, including threats (NIST, n.d.). Robustness is also described as the difference between the expected and actual behavior of a system (Taddeo 2019).

15. **Cyberspace:** A physical and virtual domain on a par with the other domains of land, sea, air, and space, which allows for human interactions and forms the Cybersecurity Economics for Emerging Markets foundation of modern life. Unlike its counterpart domains, cyberspace is entirely made by humans whose interactions form a giant grid of networks called "cyberspace," which depends on physical, logical (code), and human structures to operate. The centrality of humans in cyberspace makes social scientific approaches essential to its study. This comprehensive definition was formed by blending descriptions from academic scholars and government agencies, like the US Department of Defense, Van Puyvelde and Brantly (2019), and Demchak and Dombrowski (2013).

16. **Cyberspace layers:** The cyber persona (user), logical (code), and physical (infrastructure) layers.
17. **Disruptive cyber incident:** A cyber incident that impedes the normal operation of the targeted information systems (Harry and Gallagher 2018).
18. **Exploitive cyber incident:** A cyber incident designed to access or exfiltrate information from information systems illicitly (Harry and Gallagher 2018).
19. **Threat intelligence:** Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision- making processes (NIST, n.d.).
20. **Vulnerability:** Weakness in an information system, application, network, system security procedures, internal controls, or

implementation that could be exploited or triggered by a threat source (NIST, n.d.).

Source

CYBER SECURITY ECONOMICS FOR EMERGING MARKETS

Want to stay informed and inspired? Subscribe to our blog for insightful updates delivered straight to your inbox. Explore our website for a curated collection of reference books, resources, and more – designed to fuel your curiosity and keep you ahead.