Commentary

Cyber Security means National Security!

By: Nassim Abbas Khan | Feb 9th, 2024

IMAGE/Homeland security Today.us/

Today's world is more interconnected and globalized than ever before, with technology weaving the fabric interactions across the globe. High speed networks enabling global connectivity, sophisticated computer systems and computer-based gadgets driven by state-of-the-art software, digital data, and cutting-edge information and communication systems dominate and control our personal, organizational, and governmental interactions at national and international level. Ergo, every sphere of human activity today is driven by a global digital ecosystem with an extravagant

dependence on what we call “Cyber Space.”[1] The global digital ecosystem today is inclusive, equitable, drives conventional and digital economy, supports global supply chain, enables militaries, facilitates diplomacy, runs the national critical infrastructures, helps maintain social cohesion, promotes availability of information, and is even utilized for strategic communications. However, this digital ecosystem with its complex mesh of digital environments is extremely vulnerable where information and data lay bare on the highway of internet for cyber muggers, lurking in the hides of the digital world, to potentially jeopardize it. The most astounding development of this technological revolution is the fact that the all the elements of national power (DIME+ FIL - Diplomacy, Information, Military, Economy + Financial, Intelligence, Law enforcement) have come to extensively rely on the use of cyber space for their tactical, operational, and strategic functioning. While this reliance has incredibly facilitated and multiplied the efficiency of these elements, it has also opened new and innovative avenues for the cyber criminals, APT groups/threat actors, terrorist organizations and independent or government backed hackers to threaten the very functioning of these state elements. This exuberant reliance of all the instruments of national power on cyber space for their efficient functioning underpins the criticality of cyber security for national security necessitating a whole of the government approach to counter modern cyber threats.

The importance of cyber space is evident from the fact that it has been recognized as a domain of warfare besides land, air, sea/maritime and space and a potent cyber-attack in the cyber domain has the potential to generate catastrophic effects not only across other domains of warfare but also across the entire spectrum of state activities. It has the capability to cripple the entire economic/financial system of a country, disrupt vital communications, degrade the critical infrastructure, affect military operations, steal/destroy classified data, affect functioning of a government, and spread chaos at national and international level. In fact, cyber-attacks can be so expansive they could harm entire nations.[2] Cyber experts and scholars like Richard A. Clarke, John

Arquilla, David Ronfeldt and Peter L. Levin have predicted the inevitability of a cyberwar sooner or later which could possibly bring an entire nation down to its knees while a great many of its people are killed in the process – perhaps in the form of a 'cyber-Pearl Harbor' or 'cyber-9/11'[3]. A perfect-storm-like scenario offered by Clarke and Knake's describes a series of synchronized cyber-attacks and simultaneous crippling of the various arms of Critical National Infrastructure (CNI), the power grid, communication networks, and financial and transportation systems thus paralyzing the government with no control over the nation, military and civilian structures and potentially left vulnerable to a conventional kinetic attack (if planned like that). We may object to the very plausibility of this expansive scenario, but the recent examples of some of the famous cyber-attacks around the world do hide in them the seeds of a much wider scope and devastating consequences.

The rising threat of cyber-crimes/attacks across the globe along with the concomitant devastating material, economic, moral, reputational, social, and national security consequences are a testimony to their overwhelming capability. The 1999 cyber-attack on NASA by a teenager who stole the software controlling the international space station leaving NASA offline for 21 days, 2007 attack on Estonia which affected the government, financial system and communication networks, the 2008 attack on Georgia that dented its military command and control and left it vulnerable for a conventional attack, Stuxnet attack on the Iranian uranium enrichment facility in Natanz around 2009-10 which delayed the strategic Iranian enrichment plan by decades, 2012 attack on Saudi Aramco that wiped the data off from 30,000 computers, the attack on Ukraine's power grid in 2015 where half of the homes in the Ivano-Frankivsk region were left without power, Russia's 2017 "Not Petya" cyberattack on Ukraine, which spread across Europe, Asia, and the Americas, causing billions of dollars in damage, and the colonial pipeline ransomware attack of 2021 in the USA which led to a multi-day shutdown of the system and a ransom of $4.4 million are just few of the manifestations of the potential

of cyber-attacks at national and international level and their direct impact on the national security.

The possibility of similar attacks by individual cyber criminals or those potentially backed by a hostile government, on a larger scale anywhere in the world cannot be ruled out. The US National Cyber Security Strategy specifically names the governments of China, Russia, Iran, and North Korea to be aggressively using advanced cyber capabilities to pursue their objectives. US FBI Director Christopher Wray told Congress on 31 January 2024 that hackers backed by the Chinese government are targeting U.S. water treatment plants and electrical grids, strategically positioning themselves within critical infrastructure systems to "wreak havoc and cause real-world harm to American citizens and communities,". Likewise, experts from NATO fear that any potential cyber-attack on the Air Traffic Management system (ATM) would not only hamper the safe conduct and management of civil and military flights but could also undermine the trust in the overall security and resilience posture of the NATO and its member States.[4] Hence, any disruption of civilian aviation on a large scale would amount to national security implications thus raising the stakes to a next level across the globe. KonBriefing reported that there were 34 cyber-attacks against military setups of 26 nations across the globe in 2022 out of which 15 were NATO members including important countries like USA, UK, Turkey, France, Italy, Germany, Canada, Poland, Finland, Romania, Denmark, Estonia etc[5]. This indicates the gravity of the cyber threats for the national security of nations across the globe relying heavily on cyber space.

There is also a long list of cyber-attacks on various private and public entities which resulted in the theft of personal/classified data, stealing of personal credit card information, suspension of operations and huge financial losses for the affected companies. This trend of cyber-attacks on private commercial entities, military setups, civilian/military aviation industry continues with cyber criminals and APT groups coming up with ever evolving innovative techniques to target cyber space. According to Statista, the

worldwide cost of Cybercrimes has seen an exponential increase from 0.7 trillion dollars in 2007 to 7.08 trillion dollars per Anum in 2023. This figure is expected to reach a whooping 13.82 trillion dollars by 2028; that would be world's third biggest economy after the U.S. and China. This is largely because – unlike the days of the Cold War when only a handful of states possessed nuclear weapons – cyberattacks today may readily be carried out from both within and outside a state by a variety of state and non-state actors. At the same time, however, what makes the matter worse is the difficulty (if not the impossibility) of tracing an attack to its origin or identifying the intentions of a perpetrator behind a computer.[6] According to U.S. Cyber Security Strategy, as technological interdependencies increase and next-generation interconnectivity collapses the boundary between the digital and physical worlds, potential cost of attacks like this will only grow.[7]

The foregoing data clearly spells the criticality of cyber security in today's world and its serious national security implications necessitating persistent national level efforts to safeguard cyber space which makes the world move today. No matter how bleak the possibility of the perfect-storm scenario predicted by Clark and Knake, the devastating potential of a well-coordinated cyber-quake especially in the absence of solid/binding international cyber law[8] has forced public and private entities around the world to come up with comprehensive cyber security strategies. Today all major nations extensively dependent upon cyber space have implemented cyber laws to enforce their respective cyber security strategies. Nonetheless, ensuring cyber security is a persistent whole of government / whole of the nation effort which requires thorough understanding of the technical, operational, and strategic political aspects of the cyber space operations. Cyber criminals and those willing to exploit cyber space to harm others retain the initiative and continue to come up with ever innovative ways of attacking which makes the job of cyber defenders ever challenging, who must trace the onset of a cyber-attack/threat

as early as possible and then endeavor to contain it and minimize the damage before working towards a permanent fix.

The vulnerability of the cyber space and its possible national security implications require a well thought out national level cyber security strategy that leverages on the optimum national cyber potential to strengthen the cyber security posture and safeguard the vulnerable cyber space. Its policy guidelines must integrate the best of available human resources and cutting-edge technology through close collaboration between the private and public institutions working in the field of cyber security. The emphasis should be safeguarding the critical infrastructures of national importance while improving the overall national cyber security defenses (retaining offensive options), forging inter/intra-agency coordination, forming international partnerships and working to improve the cyber deterrence to thwart any potential threats. Last but not the least, formulation, and earnest implementation of such a wholesome cyber security strategy shall require a huge number of financial resources which must be spared and made available because cyber security means national security in today's world.

Author's Bio: Air Cdre (Retd) Nasim Abbas Khan is a senior writer and researcher at Consortium's South Asia team, Chief Strategy Officer, Privia Security, NATO and Allied forces, Istanbul, Türkiye.

---

[1] https://csrc.nist.gov/glossary/term/cyberspace. A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
[2] Clarke, R. A. & Knake, R. K., 2010. Cyber War: The Next Threat to National Security and What to do About it. New York: HarperCollins Publishers.
[3] Arquilla, J. & Ronfeldt, D., 1993. Cyberwar is Coming! Comparative Strategy, 12(1), pp. 141-165, https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/,
[4] Defending NATO's Aviation Capabilities from Cyber Attack - Joint Air Power Competence Centre (japcc.org).
[5]https://konbriefing.com/en-topics/cyber-attacks-2022-ind-military.html#Res951392.
[6] Goldsmith, J., 2013. How Cyber Changes the Laws of War. European Journal of International Law, 24(1), pp. 129-138.
[7] ibid
[8] https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763 (With few exceptions (most notably, the Budapest Convention on Cybercrime and the not-yet-in-force African Union Convention on Cyber Security and Personal Data Protection), international law does not have tailor-made rules for regulating cyberspace due to, silence, attribution, accountability, existential disagreements and interpretive issues.