Article

بسم الله الرحمن الرحيم

Global IT Updates Can Easily Be Weaponized by America to Maintain Dominance

Several weeks after the World's worst IT outage, Microsoft's cyber security partner CrowdStrike faces litigations from investors and businesses alike. The IT blackout, which occurred on July 18 and affected critical sectors worldwide including airlines, banking, healthcare providers, and television broadcasters, resulted in operational chaos and enormous economic losses.

The faulty CrowdStrike update impacted 8.5 million machines and due to the interdependence on digital ecosystems triggered systemic system failures that resulted in "blue screens of death" on Windows machines. This meant that businesses not directly impacted by the disruption were still unable to process customer transactions, e.g. airlines could not use the common ticketing system. CrowdStrike's CEO, George Kurtz confirmed that the IT fallout was because of human error, not a global cyber-attack. However, such reassurances provide little solace to businesses as they were forced to work through manual fixes on individual devices.

In fact, there is nothing new here. The World Economic Forum (WEF) has consistently categorized cyber-attacks under the broader category of cyber insecurity as a significant global risk in its annual reports. While efforts to harden defenses against cyber-attacks continue, the interdependence of global IT systems means that both wealthy and developing countries remain susceptible to criminal and terror attacks, as well as human error.

Although the CrowdStrike-induced IT disruption stemmed from human error, some management consultants and vendors have seized this opportunity to emphasize the importance of cybersecurity tools and risk management practices. For instance, McKinsey published a technocentric article focused on resilience and best-in-class cybersecurity and risk management habits. However, no one is asking the glaringly obvious question about the interconnectedness of our digital ecosystems.

What if the next global IT outage is caused by something other than conventional actors: human error, a criminal gang extorting money, a cyber-attack orchestrated by a terror group or a rogue state. The geopolitical implications of the CrowdStrike event outside normal threat actors have been largely ignored. One of the very few commentaries to consider geopolitical implications from Georgetown University was only confined to the fragility of the global technology infrastructure.

What if the United States weaponized Microsoft updates or similar services from other American companies? Such threat scenarios should raise significant concerns about global cybersecurity, trust in America's technology stack and relations between states. America has already shown its willingness to weaponize SWIFT and punish state actors such as Russia, Iran and North Korea.

Furthermore, it is widely acknowledged that major American technology companies collaborate with the Pentagon and the National Security Agency (NSA), America's premier signals intelligence organization. This partnership extends to legacy technology as well as various cutting-edge technologies, including cloud computing, artificial intelligence, augmented reality, and drones. The dual-use nature of these technologies means they have both civilian and military applications. It also implies that America could weaponize these technologies against an adversary and insulate itself through superior cyber-defenses. Imagine what would happen if Microsoft instructed its CoPilot (AI) via an update to become malicious on foreign soil. Such scenarios could have far-reaching and potentially catastrophic consequences, which could very quickly escalate into a nuclear war.

Several nations are increasingly concerned about their dependence on American technology and are actively developing sovereign technology stacks. China exemplifies this trend, working to build an entirely indigenous tech ecosystem from chips to applications, free from U.S. technology inputs. Beijing's proactive measures to shield its digital infrastructure from American big tech are evident in its resilience to events like the CrowdStrike update, achieved using domestic companies to conduct software updates. This push for technological sovereignty reflects a broader global shift towards reducing reliance on U.S.-dominated tech platforms and infrastructure.

As the world transitions towards a bipolar technological order—American versus Chinese—the Muslim world needs to standup and take note. Choosing between American or a Chinese technology translates into enslavement. Allah says in the Quran: ﴿وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ وَمِنْ رِبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُمْ وَآخَرِينَ مِنْ دُونِهِمْ لَا تَعْلَمُونَهُمُ اللَّهُ يَعْلَمُهُمْ﴾ **"And prepare against them whatever you are able of power and of steeds of war by which you may terrify the enemy of Allah and your enemy and others besides them whom you do not know [but] whom Allah knows."** [TMQ: Al Anfal:60]. This verse contains an injunction for Muslims to acquire a sovereign technological stack that gives Islam victory over its adversaries. Hence, the Muslim world is obliged to move in this direction in order to win its technological independence.

Written for the Central Media Office of Hizb ut Tahrir by

Abdul Majeed Bhatti