Cyber-politics meets the statecraft game

Bodhibrata Nag and Ranjan Pal

Voices, Tech, World, TOI

Scholars and military planners in most countries around the globe have long imagined cyberattacks as a kind of digital equivalent to nuclear war: devastating but rare. Remember the 1983 movie War Games that showcased bringing the world to a nuclear Armageddon (in those days this was cyber fiction) by hacking into military computers. Such was the amplified impact (definitely for the cautionary good) of this movie on the then US government that five presidents, starting with Reagan, set up never ending string of Washington blue-ribbon commissions to address the specter of digital destruction by nation states (e.g., Russia, China, North Korea). Apart from US, the existence of such commissions are also commonplace in many other countries today to detect, deter, and mitigate the impact of cyber-threats from political competitors.

In the wake of multiple nation-sponsored cyberattacks on societal infrastructure around the globe in the last two decades, books and research papers by academics and policymakers have conjured up images of hacked power plants and air traffic control networks, food shortages, and mass panic. While this may all be reflective of reality in certain parts of the world, cyberattacks, at best, have become a low-grade and persistent part of geopolitical competition. In other words, instead of a periodic and/or rare event, cyberattacks happen nearly every day where government representatives play a never-ending game with their competitors of espionage, deception, attack, counter-attack, destabilization, and retaliation. According to the academics mentioned above and policymakers, this is the modern form of statecraft (a theory developed by academic and political scientist Jim Bulpitt) – subtle yet causing world-changing impacts. The basic working concept of statecraft relies on the principles of signaling and shaping. To get this point across to the general audience, assume cyber-politics to be a high-stakes poker game. Here, to signal is to hint credibly at the cards one holds to influence how the other side will play its hand. Indeed, as Nobel laureate and game-theorist Thomas Schelling advocates, much of statecraft is about manipulating the shared risk of war through signaling without firing a single 'shot' and coercing a political adversary with carefully calibrated threats to gain a peaceful advantage. On the other hand, to shape is to change the state of play, stacking the deck or stealing an opponent's card for one's use. While cyber operations-driven warfare funded by international governments is increasingly influential in shaping cyber-driven geopolitics to their competitive advantage, they are comparatively ill suited for signaling a state's positions and intentions.

Hackers funded by international governments wiretap, spy, alter, sabotage, disrupt, attack, manipulate, interfere, expose, steal, and destabilize in a manner akin to a boxer who wins slowly on points rather than with a knockout blow. Hence, government-funded cyber operations are ill-suited for signaling – simply because the communication mechanism behind these operations lack calibration, credibility, and clarity. Cyber-capabilities that drive national cyber-operations are not analogous to nuclear capabilities as many policers and scholars might say, or how many government top-officials and ministers might perceive it. Most of a population, including the latter understand what nuclear weapons and tanks can do – their dependability, fungibility, or re-targetability. In contrast, the scope of possibilities, pitfalls, and methods of nation-sponsored cyber-hacking missions are comparatively opaque. Statistics (and history) has it that the nation states that benefit the most from hacking-based cyber-operations are the ones that aggressively mold the geopolitical environment to their liking using espionage (US cyber-spying on Iran's nuclear activities analogous to Soviet maskirovka, the Cayla doll introduced by USA, the Huawei chip espionage by China), sabotage (e.g., Iran uranium plant cyber-attack), and destabilization (e.g., Ukraine power grid cyber-attack) activities, rather than ones that try to diplomatically hint, coerce, or threaten their competitors (e.g., the USA-USSR Cold War activities).

In the past two decades, state-funded cyber-operations (that used to be out of public view and more a prerogative of a few nations) have scaled up to include many countries around the globe – with such operations not being private anymore. This trend perfectly fits the vision of the famed diplomat George Kennan who suggested way back in 1948 that the inevitable conflict between nation states' divergent interests would lead to a constant competition for advantage in international relations. Today, this advantage lies in manipulating civilian, business, and government resources of a country – most of which are cyber-physical in nature, Internet-connected, and rely on (competing) nation-originating (and controlling) search and social media platforms that contract with their own government and internet service providers (ISPs) to leak data on their platforms/network sourced from/about competing nations. The activities reflecting such cyber-politics do not manifest themselves in public debates at the United Nations or any other summit of international leaders or even in local, national parliamentary gatherings. Instead, the essence of such activities 'silently' flows through vast server farms, ad hoc/IoT networks of unwitting participants, third-party states, and homes and workplaces nearly everywhere. The global communications links, encryption mechanisms, internet companies, and computers that individuals use every day are the new front lines that nation-sponsored hackers are using to shape (for better or the worse) the future of statecraft.

Source: https://timesofindia.indiatimes.com/blogs/voices/cyber-politics-meets-the-statecraft-game/