With cyberattacks growing more frequent and disruptive, a unified approach is essential

June 30 2021, by Yasser Morgan

Credit: AI-generated image (disclaimer)

Cyberwarfare consists of co-ordinated attacks of mass disruption (AMD). In the June summit between U.S. and Russian presidents Joe Biden and Vladimir Putin, cyberwarfare was a topic of discussion. While the Biden-Putin summit appears to be "quite constructive," cyberwarfare

remains perplexing to politicians.

Attacks of mass disruption are similar to the latest ransomware attacks on SolarWinds and Colonial Pipeline—imagine several co-ordinated similar attacks. For the time being, organizations should prepare for increasing disruptions and data losses caused by ransomware.

Attacks of mass disruption may not cause massive casualties, but nations could lose their ability to function and respond to adversaries, economies can be crippled and governments may be undermined. The 2015 cyberattack on Ukraine presented a scenario of grounding a nation using a well co-ordinated cyberattack.

The lessons are clear—the impact of cyberattacks is too serious to ignore and pre-planned contingencies may be the only thing that works to address them.

Cyberattack losses

In 2020, IBM estimated US$1.5 billion losses in known observed cyberattacks.

Over the past two decades, two factors have contributed to the possibility of cyberwarfare. First is the increased reliance on digital infrastructure and systems. Second is the continuous increase in damages inflicted by criminal or state-based cyberattacks.

These provide sufficient justification for experts to sound the alarm on cybersecurity.

Other factors increase the risks even more. The complexity of the modern economy and its supply chains create an environment of highly impactful disruptions. Attacks of mass disruption on seemingly

irrelevant but well-selected entities—like infrastructure companies—could trigger a domino effect that causes disruptions and economic losses far beyond the scale of the target.

Russia used U.S. cyberinfrastructure to influence the 2016 election. In May 2021, there were attacks on software developer SolarWinds Inc., oil infrastructure company Colonial Pipeline and JBS, the world's largest meat supplier.

Currently, most cyberattacks originating from Russia use known tactics like email phishing, ransomware-as-a-service and poor password practices.

Treaty challenges

A zero-day vulnerability occurs the first time the vulnerability is exploited, like when the malicious program Stuxnet was successfully used as a digital "dirty bomb" to curb Iranian nuclear ambition.

The U.S. is known to exploit hardware vulnerabilities through highly sophisticated, maintaining the the upper hand in the ability to perform silent attacks.

Calls to bring governments together to sign a treaty similar to other arms-control treaties have mounted lately. To address the complexities of cyberwarfare, political scientist Joseph Nye and others have proposed a nuclear-like treaty, in particular, due to the ability of nuclear treaties to precisely spell out details.

Most efforts to control attacks of mass disruption have either led to limited scope agreements, or completely fallen apart before they were signed.

Unfortunately, cyberattacks do not use observable weapons that can be monitored for compliance. Further, the fine line between criminal and state-based attacks could be hard to distinguish. An attack on a gas pipeline or a meat-packing facility may appear criminal, but can trigger serious chain events beyond the immediate targets.

The rapid technological changes and advances in cyberattacks make it hard to predict the strategies of future attacks of mass disruption in order to address them in a treaty.

Protecting against attacks

Most attacks of mass disruption exploit vulnerabilities that are easy to fix by maintaining normal digital hygiene and a vigilant attitude to email phishing and password management.

Organizations need to get serious about those practices because, like COVID-19, vigilant proactive precautions can lessen the problem to a great extent.

Protective measures can be imposed through national legislation. A national debate is required to develop consensus on the level of government intervention and the levels of protections for different data types. This should result in a call for strong legislation forcing organizations to maintain high levels of security like off-site backups and other protective measures.

Deep vulnerabilities embedded deep into hardware and operating systems, on the other hand, cannot be mitigated by normal digital hygiene. The U.S. has the upper hand on those vulnerabilities, hence, the cybersecurity arms balance is tilted in favour of the U.S.

Historically, nations do not settle arms race until a mutual assured

destruction situation presents itself. Russian cyberattacks could be viewed as an attempt to reach this point. Until we get closer to the mutual assured destruction point, do not expect an international treaty anytime soon. Instead, expect more cyberattacks and data losses. Organizations and governments need to get serious and buckle up—it's going to be a rough ride.

Provided by The Conversation