Source : www.thehindu.com Date : 2021-02-11

DISINFORMATION IS A CYBERSECURITY THREAT

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Cybersecurity focuses on protecting and defending computer systems, networks, and our digital lives from disruption. Nefarious actors use attacks to compromise confidentiality, the integrity and the availability of IT systems for their benefit. Disinformation is, similarly, an attack and compromise of our cognitive being. Nation-state actors, ideological believers, violent extremists, and economically motivated enterprises manipulate the information ecosystem to create social discord, increase polarisation, and in some cases, influence the outcome of an election.

There is a lot of similarity in the strategies, tactics and actions between cybersecurity and disinformation attacks. Cyberattacks are aimed at computer infrastructure while disinformation exploits our inherent cognitive biases and logical fallacies. Cybersecurity attacks are executed using malware, viruses, trojans, botnets, and social engineering. Disinformation attacks use manipulated, miscontextualised, misappropriated information, deep fakes, and cheap fakes. Nefarious actors use both attacks in concert to create more havoc.

Also read | Cybersecurity trends turned unpredictable after COVID-19, says PwC

Historically, the industry has treated these attacks independently, deployed different countermeasures, and even have separate teams working in silos to protect and defend against these attacks. The lack of coordination between teams leaves a huge gap that is exploited by malicious actors.

Cognitive hacking is a threat from disinformation and computational propaganda. This attack exploits psychological vulnerabilities, perpetuates biases, and eventually compromises logical and critical thinking, giving rise to cognitive dissonance. A cognitive hacking attack attempts to change the target audience's thoughts and actions, galvanise societies and disrupt harmony using disinformation. It exploits cognitive biases and shapes people by perpetuating their prejudices. The goal is to manipulate the way people perceive reality. The storming of the U.S. Capitol by right-wing groups on January 6, 2021, is a prime example of the effects of cognitive hacking.

The implications of cognitive hacking are more devastating than cyberattacks on critical infrastructure. The damage wrought by disinformation is challenging to repair. Revolutions throughout history have used cognitive hacking techniques to a significant effect to overthrow governments and change society. It is a key tactic to achieve major goals with limited means.

Also read | '42% of firms will continue to invest in cybersecurity'

For example, QAnon spread false information claiming that the U.S. 2020 presidential election was fraudulent, and conspiracy theorists (in the United Kingdom, the Netherlands, Ireland, Cyprus and Belgium) burned down 5G towers because they believed it caused the novel coronavirus pandemic. COVID-19 disinformation campaigns have prevented people from wearing masks, using potentially dangerous alternative cures, and not getting vaccinated, making it even more challenging to contain the virus.

Distributed Denial-of-Service (DDoS) is a well-coordinated cybersecurity attack achieved by flooding IT networks with superfluous requests to connect and overload the system to prevent legitimate requests being fulfilled. Similarly, a well-coordinated disinformation campaign fills broadcast and social channels with so much false information and noise, thus taking out the

system’s oxygen and drowning the truth.

The advertisement-centric business modes and attention economy incentivise malicious actors to run a sophisticated disinformation campaign and fill the information channels with noise to drown the truth with unprecedented speed and scale.

Also read | U.S. cybersecurity agency warns of ‘grave threat’ to computer networks

Disinformation is used for social engineering threats on a mass scale. Like phishing attacks, to compromise IT systems for data extraction, disinformation campaigns play on emotions, giving cybercriminals another feasible method for scams.

A report released by Neustar International Security Council (NISC) found 48% of cybersecurity professionals regard disinformation as threats, and of the remainder, 49% say that threat is very significant; 91% of the cybersecurity professionals surveyed called for stricter measures on the Internet.

Deep fakes add a whole new level of danger to disinformation campaigns. A few quality and highly targeted disinformation campaigns using deepfakes could widen the divides between peoples in democracies even more and cause unimaginable levels of chaos, with increased levels of violence, damage to property and lives.

Also read | Only 20% of Indians are not confident in their ability to prevent a cyber attack

Cybersecurity experts have successfully understood and managed the threats posed by viruses, malware, and hackers. IT and Internet systems builders did not think of security till the first set of malicious actors began exploiting security vulnerabilities. The industry learned quickly and invested profoundly in security best practices, making cybersecurity a first design principle. It developed rigorous security frameworks, guidelines, standards, and best practices such as defense-in-depth, threat modelling, secure development lifecycle, and red-team-blue-team (self-attack to find vulnerabilities to fix them) to build cybersecurity resilience. ISACs (Information sharing and analysis centers) and global knowledge base of security bugs, vulnerabilities, threats, adversarial tactics, and techniques are published to improve the security posture of IT systems.

We can learn from decades of experience in the cybersecurity domain to defend, protect and respond, and find effective and practical solutions to counter and intervene in computational propaganda and infodemics. We can develop disinformation defence systems by studying strategy and tactics to understand the identities of malicious actors, their activities, and behaviours from the cybersecurity domain to mitigate disinformation threats. By treating disinformation as a cybersecurity threat we can find effective countermeasures to cognitive hacking.

Also read | Have you completed your cybersecurity homework?

Defense-in-depth is an information assurance strategy that provides multiple, redundant defensive measures if a security control fails. For example, security firewalls are the first line of defence to fend off threats from external systems. Antivirus systems defend against attacks that got through the firewalls. Regular patching helps eliminate any vulnerabilities from the systems. Smart identity protections and education are essential so that users do not fall victim to social engineering attempts.

We need a defense-in-depth strategy for disinformation. The defense-in-depth model identifies

disinformation actors and removes them. Authenticity and provenance solutions can intervene before disinformation gets posted. If the disinformation still gets by, detection solutions using humans and artificial intelligence, internal and external fact-checking can label or remove the content.

Today, the response to disinformation is in silos of each platform with little or no coordination. There is no consistent taxonomy, definitions, policy, norms, and response for disinformation campaigns and actors. This inconsistency enables perpetrators to push the boundaries and move around on platforms to achieve their nefarious goals. A mechanism like ISACs to share the identity, content, context, actions, and behaviours of actors and disinformation across platforms is needed. Information sharing will help disinformation countermeasures to scale better and respond quickly.

A critical component of cybersecurity is education. Technology industry, civil society and the government should coordinate to make users aware of cyber threat vectors such as phishing, viruses, and malware. The industry with public-private partnerships must also invest in media literacy efforts to reach out to discerning public. Intervention with media education can make a big difference in understanding context, motivations, and challenging disinformation to reduce damage. The freedom of speech and the freedom of expression are protected rights in most democracies. Balancing the rights of speech with the dangers of disinformation is a challenge for policymakers and regulators. There are laws and regulations for cybersecurity criminals. More than 1,000 entities have signed the Paris Call for Trust and Security in Cyberspace, for stability and security in the information space. Similarly, 52 countries and international bodies have signed the Christchurch Call to Action to eliminate terrorist and violent extremist content online.

Also read | Why cybersecurity should be a part of the regular IT curriculum

The disinformation infodemic requires a concerted and coordinated effort by governments, businesses, non-governmental organisations, and other entities to create standards and implement defences. Taking advantage of the frameworks, norms, and tactics that we have already created for cybersecurity is the optimum way to meet this threat. We must protect our society against these threats or face the real possibility of societal breakdown, business interruption, and violence in the streets.

Ashish Jaiman, a technologist and innovator, is the Director of Technology and Operations for the Customer Security and Trust organisation at Microsoft

We brief you on the latest and most important developments, three times a day.

*Our Digital Subscription plans do not currently include the e-paper, crossword and print.

Dear reader,

We have been keeping you up-to-date with information on the developments in India and the world that have a bearing on our health and wellbeing, our lives and livelihoods, during these difficult times. To enable wide dissemination of news that is in public interest, we have increased the number of articles that can be read free, and extended free trial periods. However, we have a request for those who can afford to subscribe: please do. As we fight disinformation and misinformation, and keep apace with the happenings, we need to commit greater resources to news gathering operations. We promise to deliver quality journalism that stays away from vested interest and political propaganda.

Dear subscriber,

Thank you!

Your support for our journalism is invaluable. It’s a support for truth and fairness in journalism. It has helped us keep apace with events and happenings.

The Hindu has always stood for journalism that is in the public interest. At this difficult time, it becomes even more important that we have access to information that has a bearing on our health and well-being, our lives, and livelihoods. As a subscriber, you are not only a beneficiary of our work but also its enabler.

We also reiterate here the promise that our team of reporters, copy editors, fact-checkers, designers, and photographers will deliver quality journalism that stays away from vested interest and political propaganda.

Suresh Nambath

Please enter a valid email address.

You can support quality journalism by turning off ad blocker or purchase a subscription for unlimited access to The Hindu.

Sign up for a 30 day free trial.

END