



Resilient Governance: Cybersecurity Strategy for the Public Sector

Presented to Officials at Nepali Administrative Staff College on 11th May 2026

Rajib Subba, PhD

ABOUT 2500 YEARS AGO



**“All warfare
is based on
deception.”**

Sun Tzu (The Art of War)

Today, deception manifests through phishing, fraud, false transactions, and manipulation in digital sphere.

WHAT IS THE RELATIONSHIP BETWEEN BEER & DIAPER?



Significance of IT!

- ▶ Tell me one area in your life that is not touched by IT!
- ▶ IT encompass every sector of society!
- ▶ IT is fastest growing field!
- ▶ 80,000 - 100,000 jobs by 2025 in Nepal.
- ▶ IT has future implications!
 - ▶ Bank to eBank
 - ▶ eHealth
 - ▶ eEducation
 - ▶ Virtual World
 - ▶ Crypto and Blockchain
 - ▶ IoT



Regular ATM and Bitcoin ATM

Three vital roles of ICT/IT/IS

- ▶ Support of business processes and operations
 - ▶ Examples are sales transactions, inventory ordering, and payroll processing.
 - ▶ DM Example: Disaster Logistics for relief distribution
- ▶ Support of decision making by employees and managers
 - ▶ Information systems can support managers in decision making process by providing them with useful information on demand.
 - ▶ For example stock exchange, fuel price [on demand]
 - ▶ DM Example: Immediate rescue with location of GIS data
- ▶ Support of strategies for competitive advantage
 - ▶ Information systems can make available new types of products and services through which an organization might gain a competitive advantage. [Dell Computers]
 - ▶ PubAdmin Example: Outreach with social media

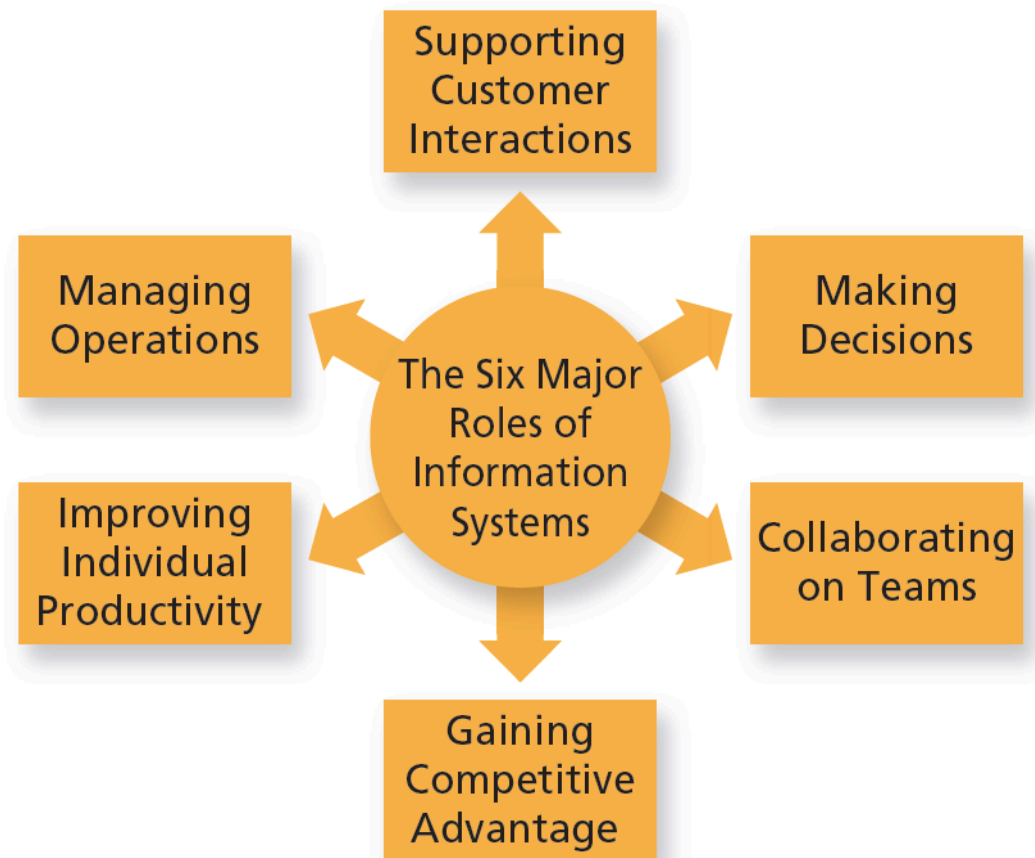
How do you use technology to improve your productivity?

	Not at All True for Me					Very True for Me	
1. I empty my email inbox every day.	1	2	3	4	5	6	7
2. I keep a to-do list, and always keep it up to date.	1	2	3	4	5	6	7
3. I use email filters to sort messages by how important they are.	1	2	3	4	5	6	7
4. I stay logged into my social network most of the day so I am alerted when updates occur or messages appear.	1	2	3	4	5	6	7
5. I rarely print anything out.	1	2	3	4	5	6	7
6. I send and receive text messages very frequently, though most are unimportant.	1	2	3	4	5	6	7
7. I focus on the most important projects and can ignore distractions.	1	2	3	4	5	6	7
8. I have a clear vision of what I want to achieve and make priorities.	1	2	3	4	5	6	7
9. I keep my calendar online rather than on paper, and I keep it up to date.	1	2	3	4	5	6	7
10. My electronic files are very well organized.	1	2	3	4	5	6	7

Result

- ▶ To find your score, add up the numbers for all questions except 4 and 6. For those two questions, first reverse the score by giving yourself 1 point if you chose 7, 2 points if you chose 6, and so on.
- ▶ Then add the reversed score to your total.
- ▶ If your total is higher than 50, you have some good habits that are associated with high productivity, including the use of information systems that can help you streamline.

Major roles of IT/ICT/IS for organizations



1. Making Decisions

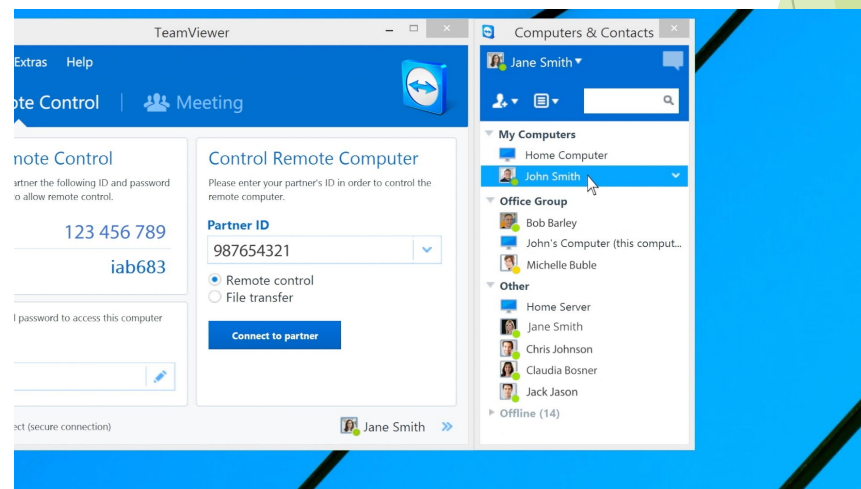
- ▶ 40% Executives trust their guts. (Wailgum, 2009) CIO.com
- ▶ Data-driven decision making helps to understand trends and patterns. **Example:** Beer and Diaper
- ▶ Source of information can be internal and external.
- ▶ Business intelligence help Managers utilize information from many sources.
 - ▶ **Example:** online buying pattern



2. Collaborating on Teams

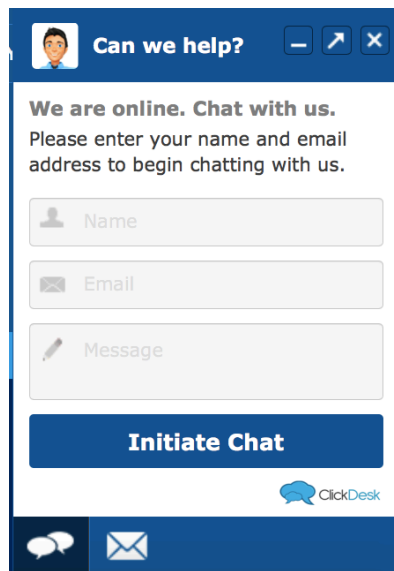
- ▶ Information systems allow people to work together at any time and from any place.
- ▶ Conduct online meetings, share files/documents and applications and interact virtually.
- ▶ Examples:

- ▶ Social networks
- ▶ Online communities
- ▶ SharePoint
- ▶ Salesforce
- ▶ Team Viewer
- ▶ Google Docs

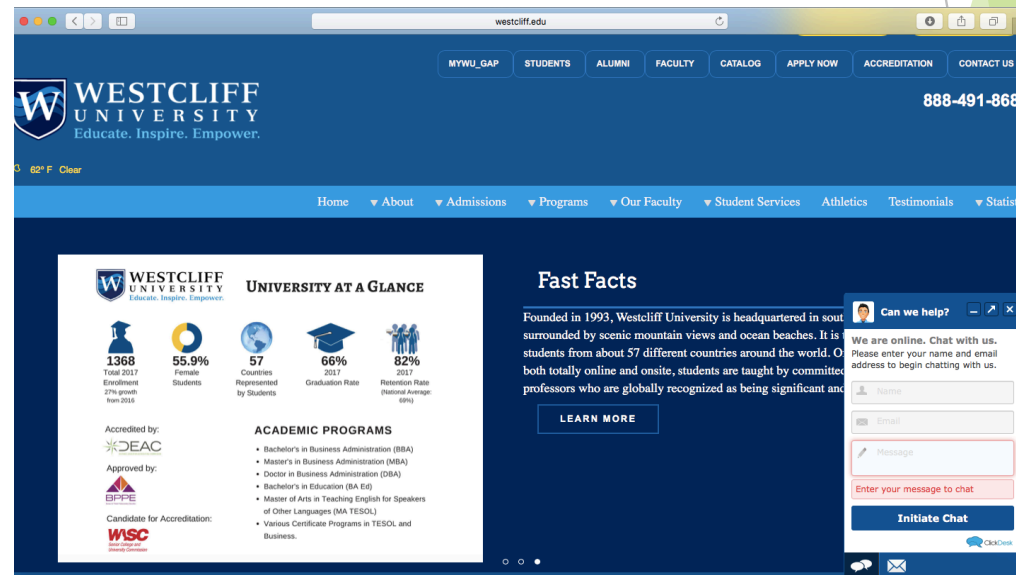


3. Customer Interactions

- ▶ Beer and Diaper: Customer Experience?
- ▶ CRM systems build and maintain relationships.
- ▶ Web-based front offices and online self-service.
- ▶ Example: Chat bot



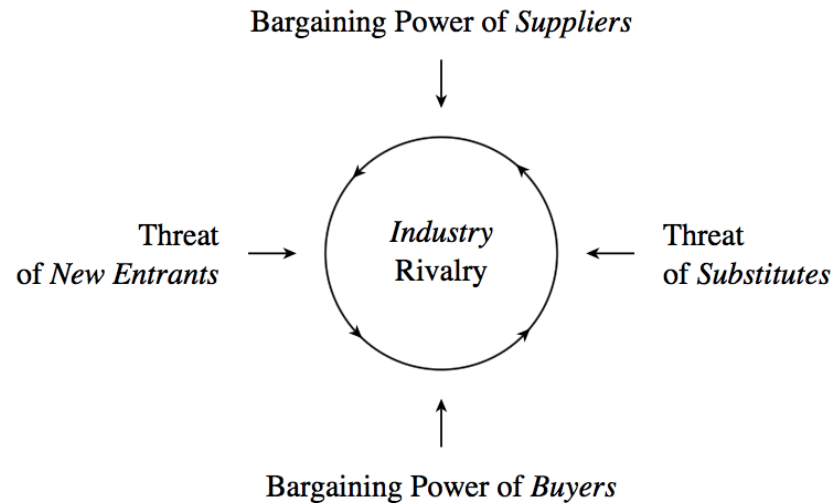
A screenshot of a chat widget interface. At the top, it says "Can we help?" with a minus, plus, and close button. Below that, it says "We are online. Chat with us. Please enter your name and email address to begin chatting with us." There are three input fields: "Name", "Email", and "Message". At the bottom, there is a blue button labeled "Initiate Chat" and a ClickDesk logo.



A screenshot of the Westcliff University website. The header includes the university logo, name, and tagline "Educate. Inspire. Empower." along with a phone number "888-491-8686". The navigation bar lists various links: MYWU_GAP, STUDENTS, ALUMNI, FACULTY, CATALOG, APPLY NOW, ACCREDITATION, and CONTACT US. The main content area features a "UNIVERSITY AT A GLANCE" section with statistics: 1368 Total 2017 Enrollment (27% growth from 2016), 55.9% Female Students, 57 Countries Represented by Students, 66% 2017 Graduation Rate, and 82% 2017 Retention Rate (National Average 69%). It also lists academic programs and accreditation details. A "Fast Facts" section on the right mentions the university's founding in 1993 and its location. A chat widget is overlaid on the bottom right, identical to the one in the previous image.

4. Strategic Objectives

- ▶ Competitive advantage gives a firm a lead over it's rival.
- ▶ Porter's five forces model?



Managing Operations

Suppose
transport
How do



Example: UPS drivers, for instance, know to avoid left turns on their delivery routes when possible, because they take a few seconds longer, wasting time and gas.

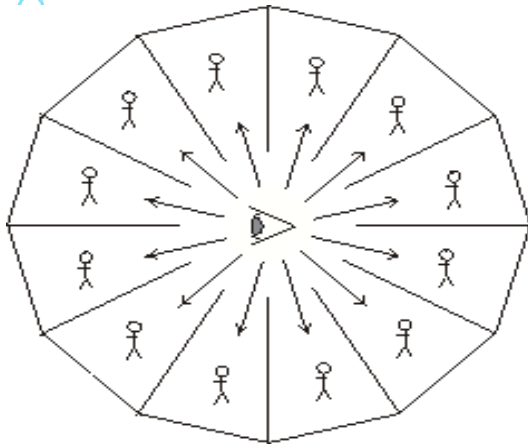
5. Managing Operations

- ▶ Functions to deliver goods and services
- ▶ Industry-specific operations such as these:
 - ▶ Transportation companies rely on information systems equipped with GPS to track their fleets, optimize routes, and conserve gas. **Example:** Fleet MGMT
 - ▶ Manufacturers need systems to manage assembly lines, product quality, production schedules, and **just-in-time** supply deliveries. **Example:** Toyota, Pizza Delivery
 - ▶ **Colleges and universities** need systems to manage student academic records, class scheduling, faculty assignments, and student financial aid.
 - ▶ Companies that buy products from suppliers around the globe need **real-time updates** on their global supply chains to manage inventories and reduce costs. **Example:** Walmart
- **Advantages:**
 - ▶ Achieving excellence in operations can provide **enormous cost savings** without sacrificing quality **competitive advantage**.

6. Individual Productivity

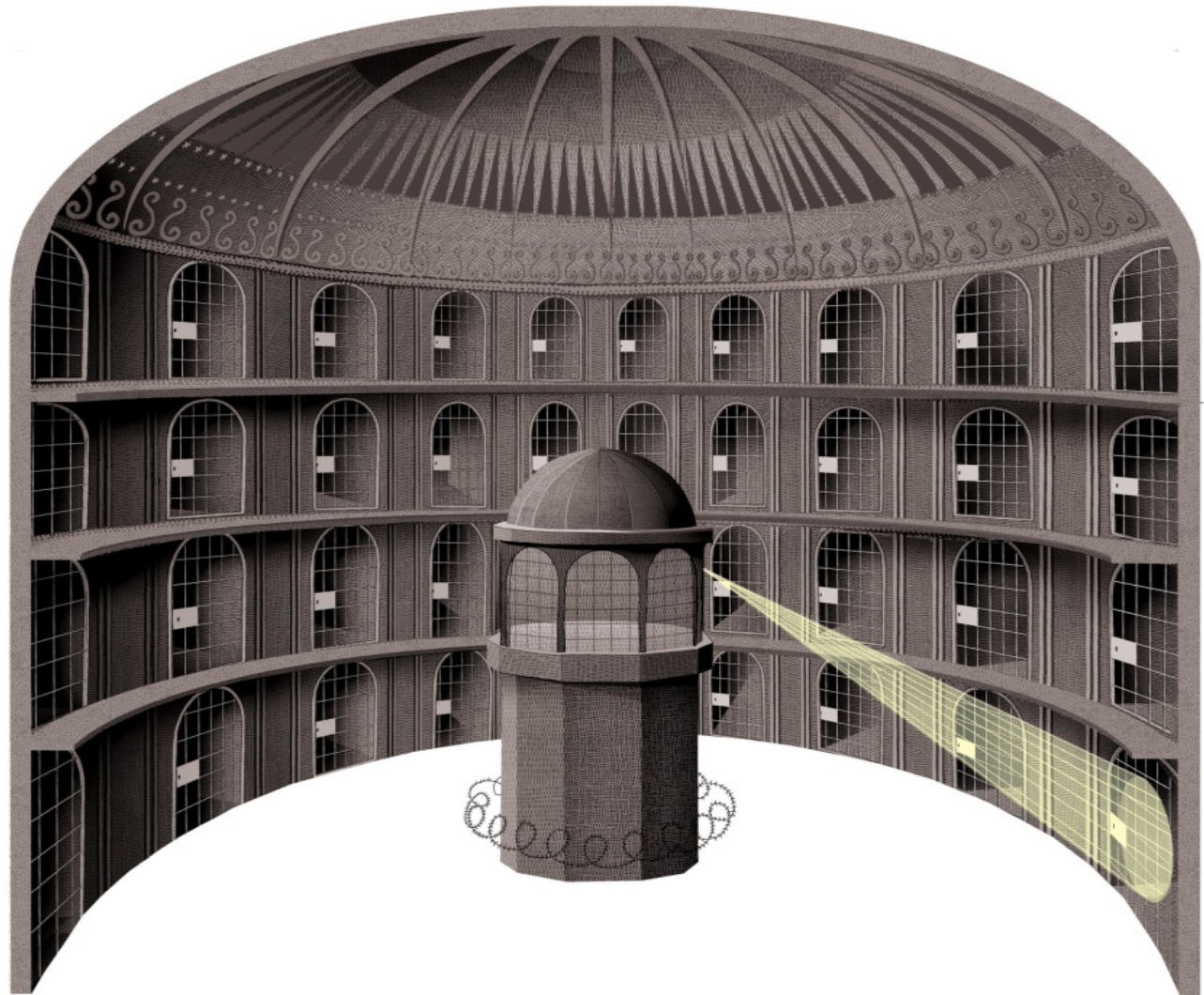
- ▶ You need to write a report with a large number of references!
How do you automatically create and properly format your term paper references? How do you efficiently manage your bibliography?
- ▶ Use
 - ▶ Computer software
 - ▶ Electronic devices
- ▶ Example:
 - ▶ Bibliographic Manager
 - ▶ EndNote and RefNote





The scheme of this design was to allow single person to watch over inmates without them being able to tell whether or not they are being watched.

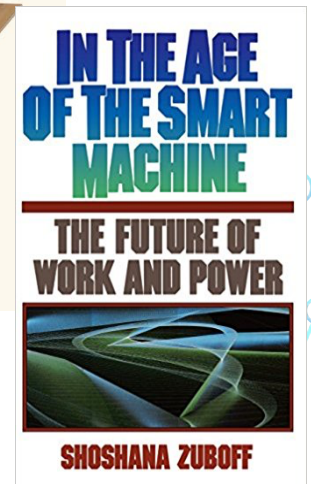
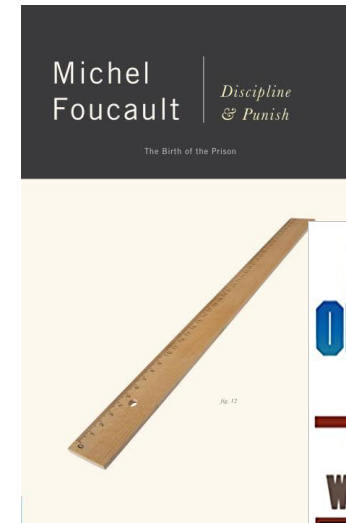
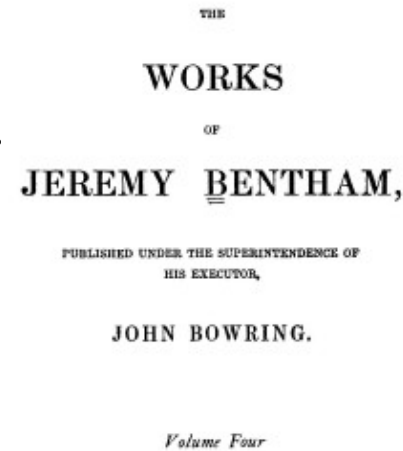
This means that all inmates must act as though they are watched at all times, effectively controlling their own behavior constantly.



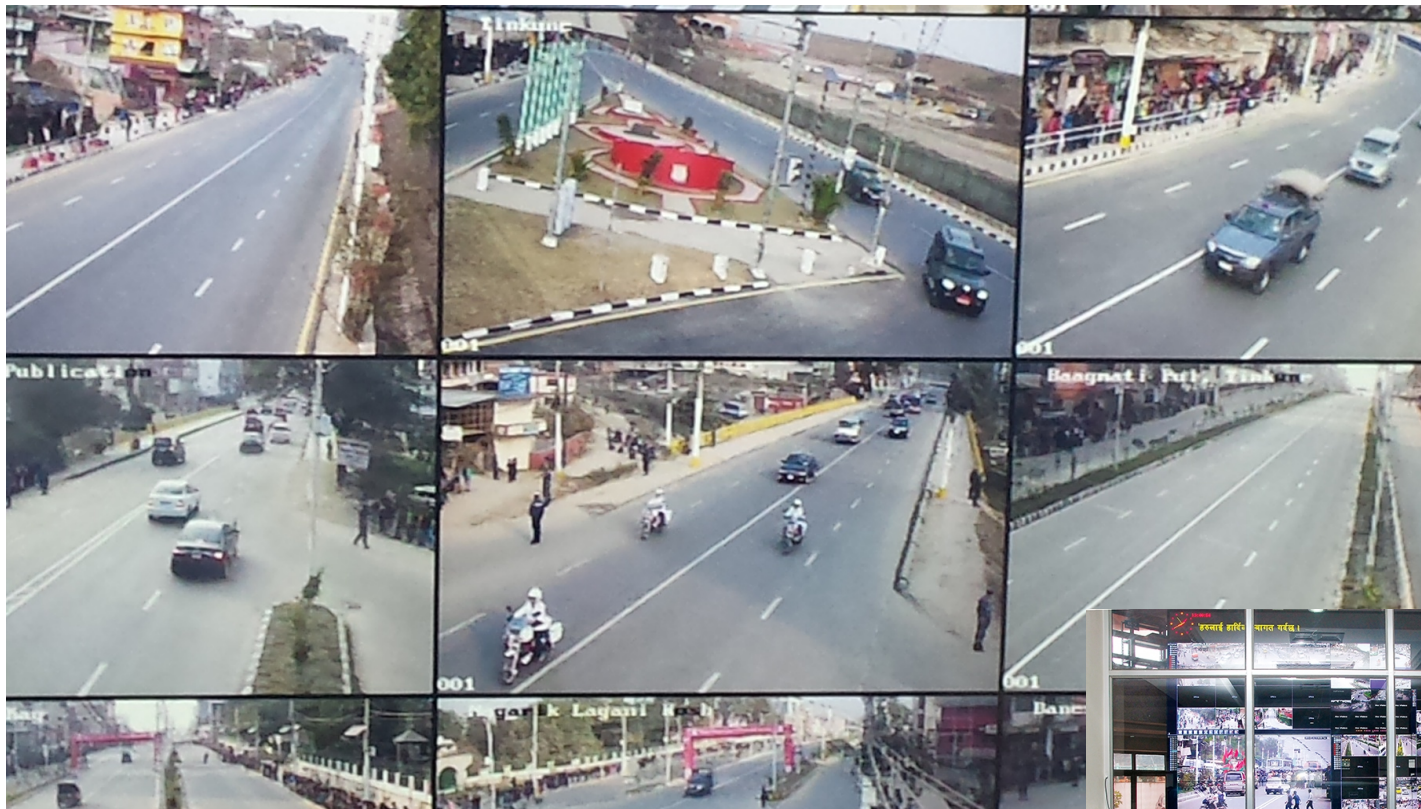
PANOPTICON



- This concept is called panopticon.
- Which came from the Greek means '**all**' and **seeing**.
- Concept developed by **Jeremy Bentham** in 18th Century.
- **Michel Foucault** in 1975 suggested, inmates are always "the object of information".
- This concept was further theorized as **"Information Panopticon"** by Shoshana Zuboff (In the Age of the Smart Machine, 1988).
- **Information Panopticon:**
 - Information and Communication Technologies as observational tools for decision making.



E-PANOPTICON IN ACTION



18th SAARC Summit Joint Command Center, Nepal Army HQs



CYCLONE AMPHAN IN BANGLADESH

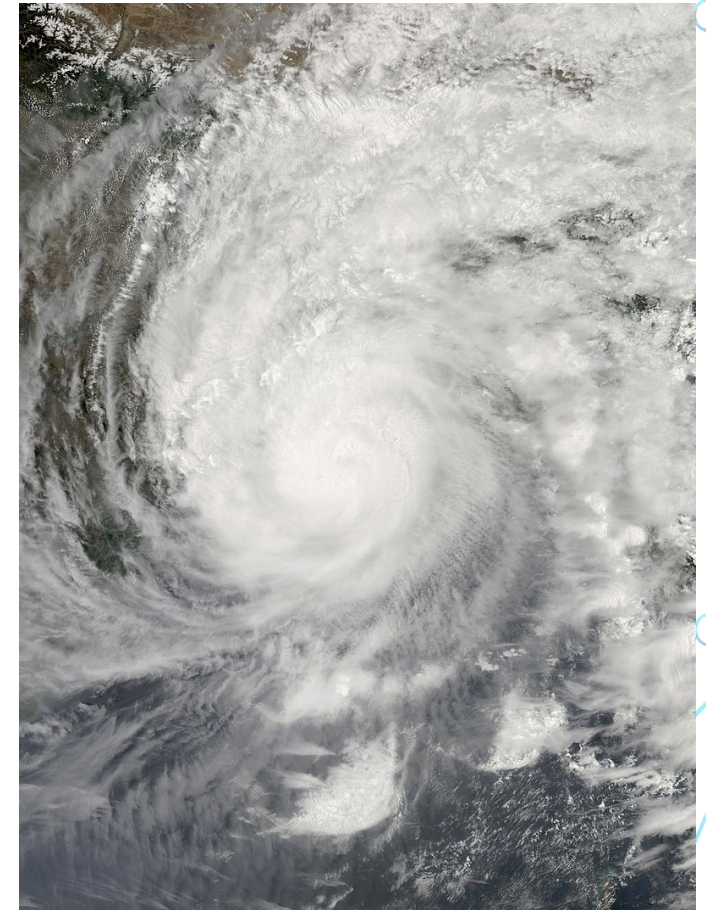
Cyclone Amphan in May 2020 killed 26 people.
Evacuated: Nearly 2 million people.

In contrast:

- November 1970 cyclone killed 300,000 people.
- 1991 cyclone killed 145,000.

WMO:

- high resolution numerical weather prediction info.
- round clock surveillance of tropical cyclones by satellites (three satellites over the Bay of Bengal)
- a network of Radars and a denser network of weather stations, and exchange of those data.



Break!





CYBER THREATS: DARK SIDE OF DIGITAL INNOVATION

- Cyber Threats are real and pertinent to security including financial security.
- Attacks, now, don't need physical weapons as trends of cyber operations, which can be **deniable and unattributable**, are **increasing** and getting **lethal**. [US DNI, 2013].
- **UN Secretary-General Antonio Guterres, July 2018**
 - “Dark side of digital innovation”.
 - Formed a High-Level Panel on Digital Cooperation, to address the dark side of innovation -- such as cybersecurity threats, the risks of cyberwarfare, the magnification of hate speech, and violations of privacy.
- Cyber threats are no longer the purview of computer sector.





In 1697, Dutch explorers led by Willem de Vlamingh became the first Europeans to see black swans, in Western Australia.

Black swan is about unknown unknowns....one of the four paradigm of risks!



TYPES OF RISKS

Known Knowns

Things we are aware of
and understand.

Known Unknowns

Things we are aware of but
don't understand.

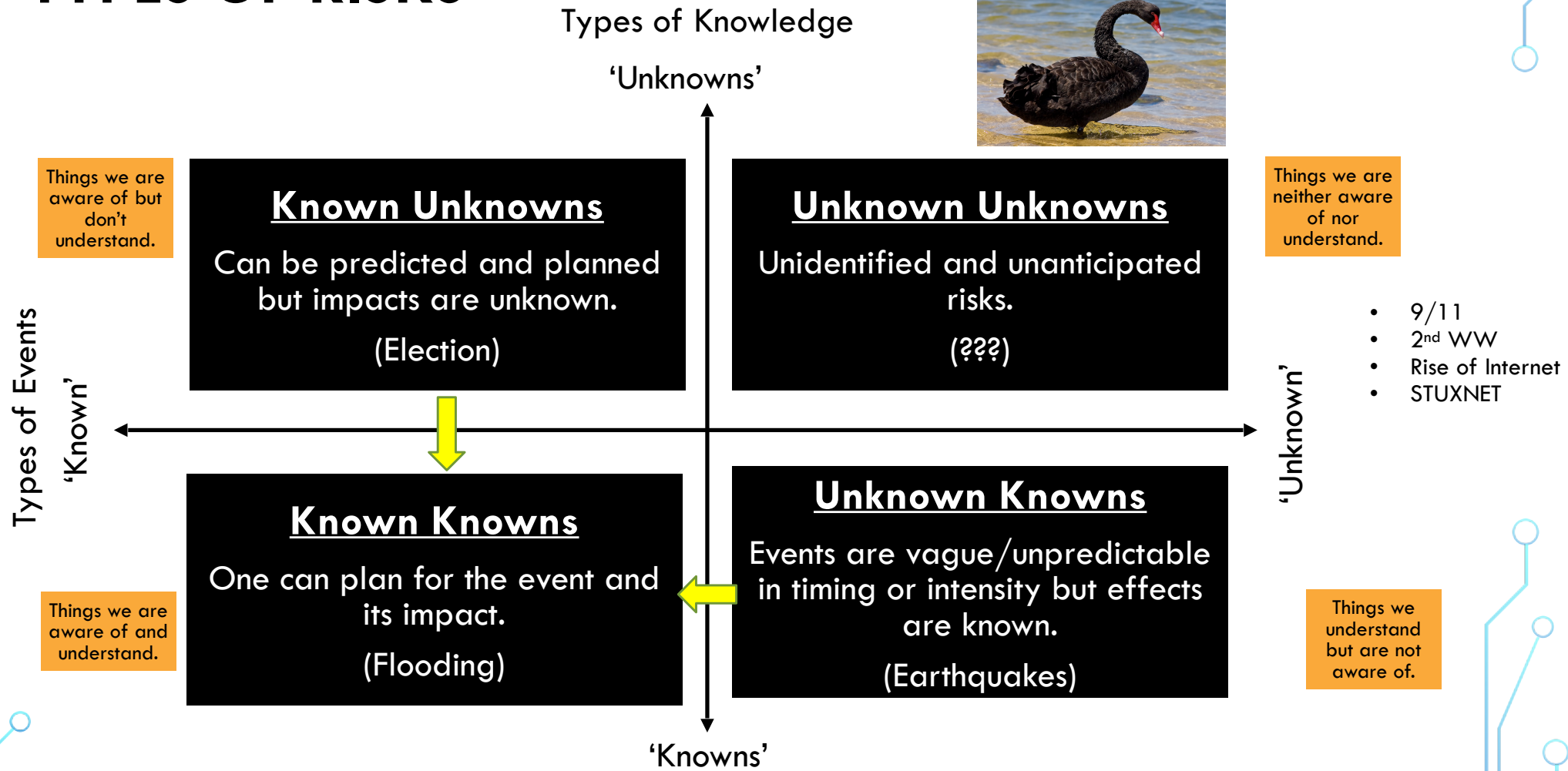
Unknown Knowns

Things we understand but are
not aware of.

Unknown Unknowns

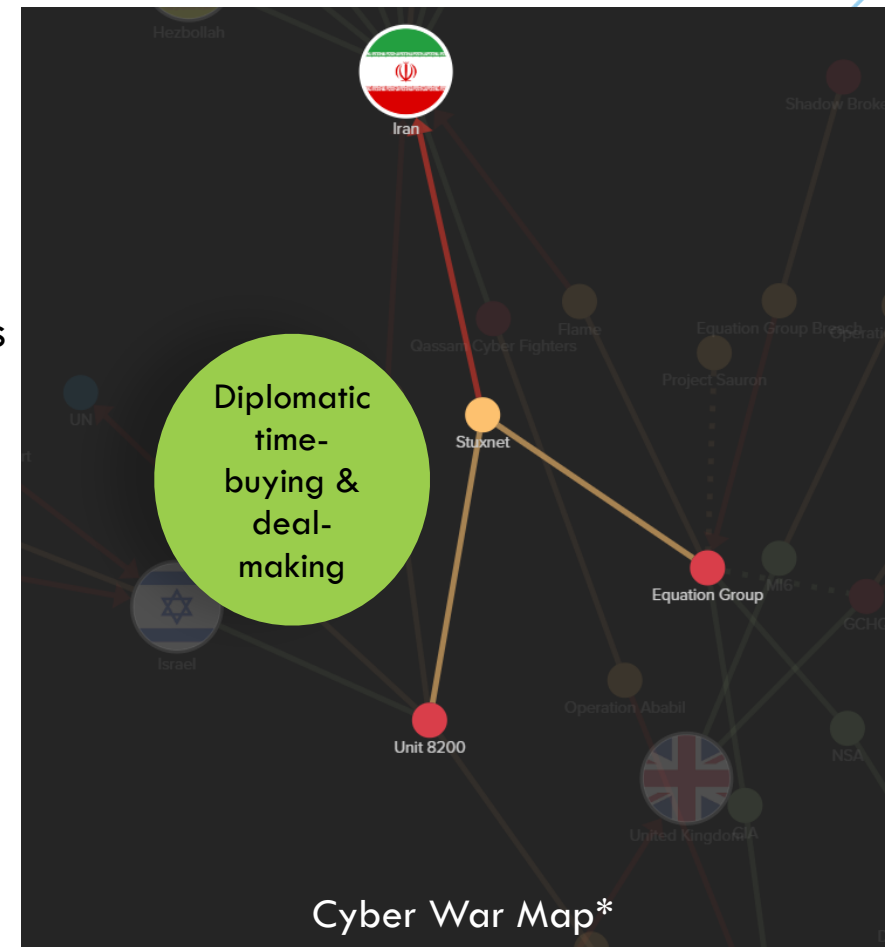
Things we are neither
aware of nor understand.

TYPES OF RISKS



STUXNET: CYBER WEAPON

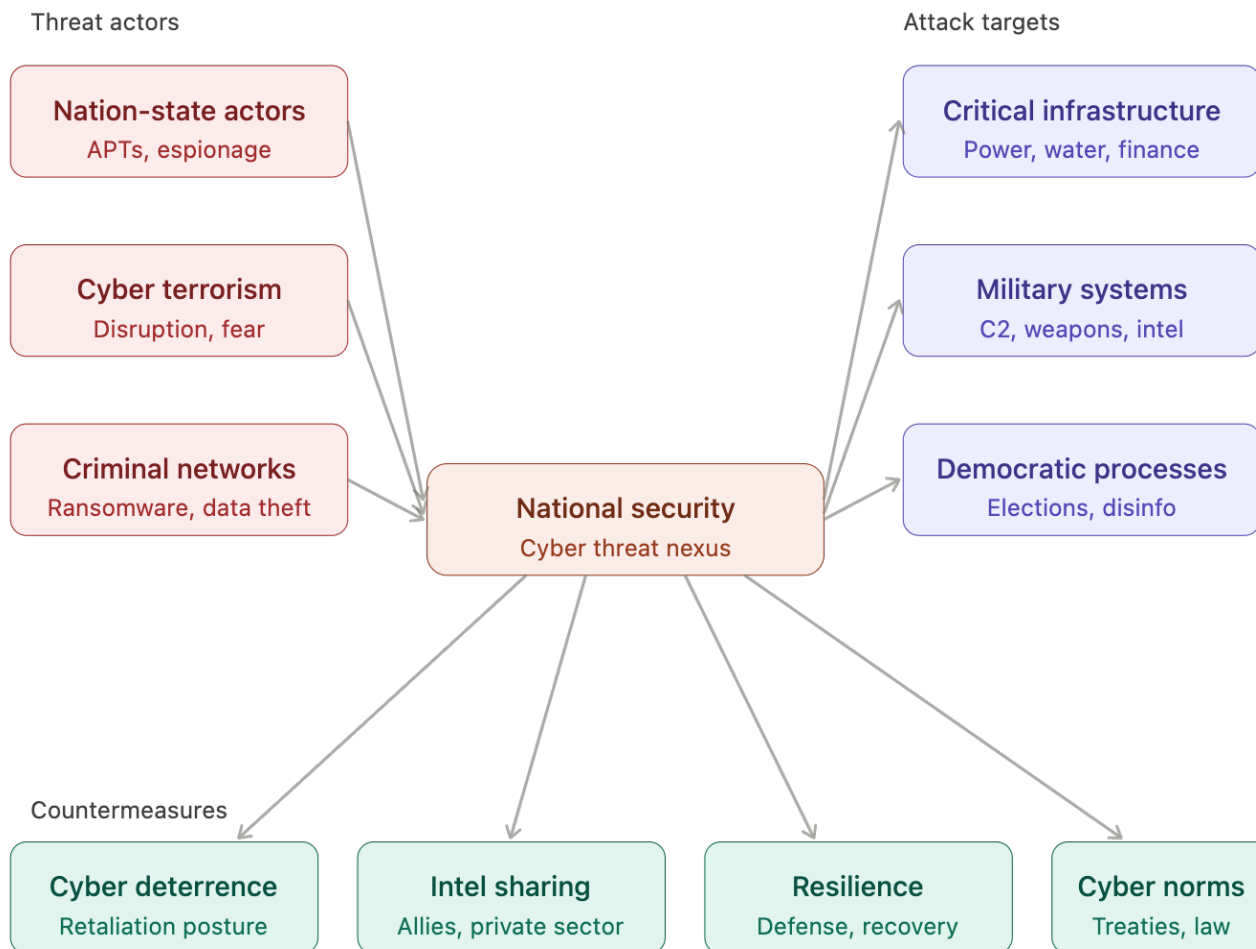
- January 2010. Officials of International Atomic Energy Agency (IAEA) noticed faster degradation of nuclear centrifuges at a uranium enrichment plant in Iran.
- June 2010: A unique “virus” was discovered in computers of Iranian nuclear plant. This virtual weapon became instrumental for nuclear deal between Iran and other countries in 2013.
- *Zero-day exploit*: Software vulnerabilities that are still unknown to software maker and to antivirus vendors - which means there are no antivirus signature and no patches available to fix the holes.



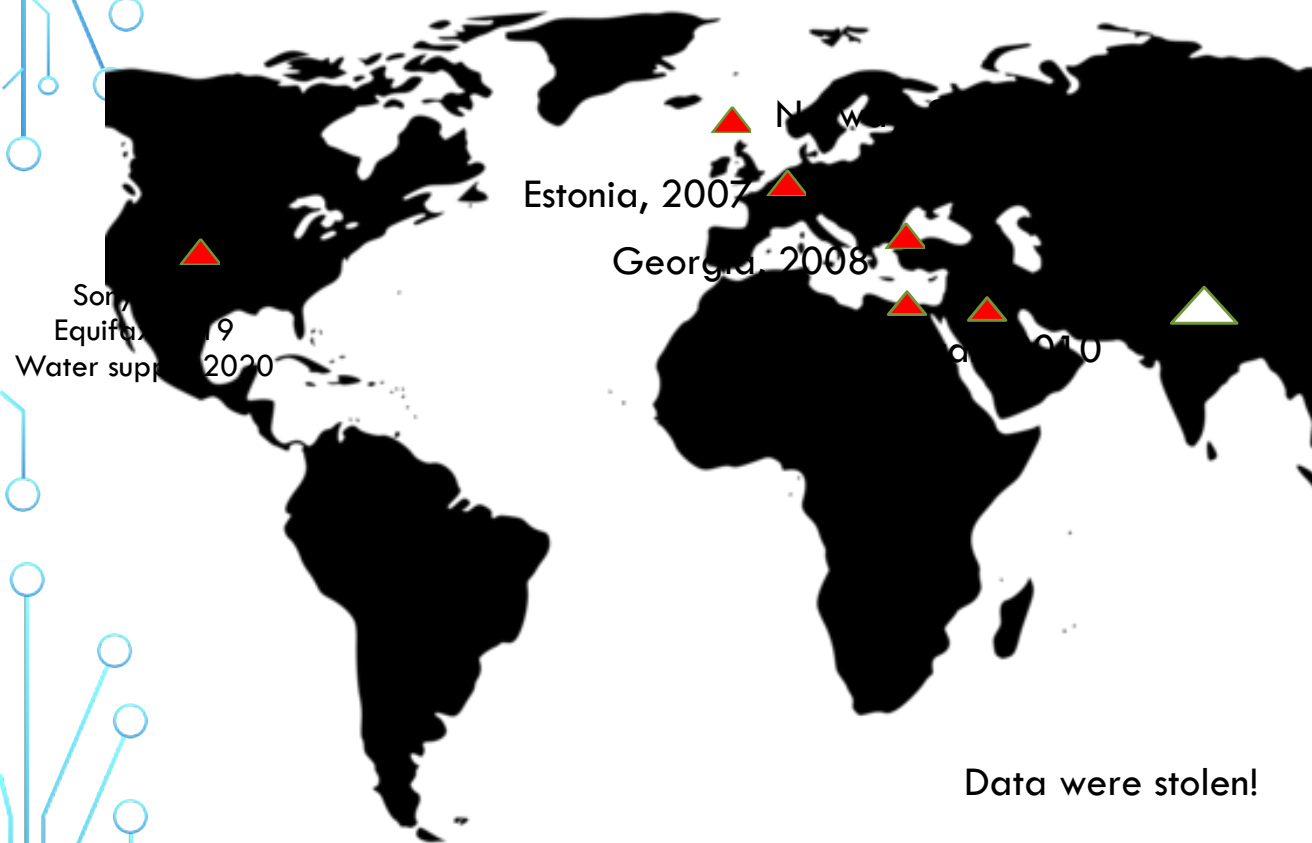
*<https://embed.kumu.io/0b023bf1a971ba32510e86e8f1a38c38#apt-index>

THREAT LANDSCAPE

- APT: Advanced Persistent Threat
- C2: Command and Control



MAJOR CYBER ATTACKS OF RECENT TIMES



Kaplan F (2016) Kello, L. (2017)

Crippled critical infrastructure.

After paralyzing critical infrastructure tanks rolled in.

Stuxnet: Zero-day exploit.

Stole data from corporations or force closure. Cost: \$58 M

Actors: Patriotic hackers.

“State-sponsored”

Non-attributable acts

MAJOR CYBER ATTACKS OF RECENT TIMES

Estonia, April, 2007 (Kaplan, 2015)

- Estonia was hit with a massive cyber attack, its networks and servers flooded with so much data that they shut down.
- “This attack persisted and was followed up—in **three separate waves**—with infections of malware that spread from one computer to another, across the tiny nation, in all spheres of life”.

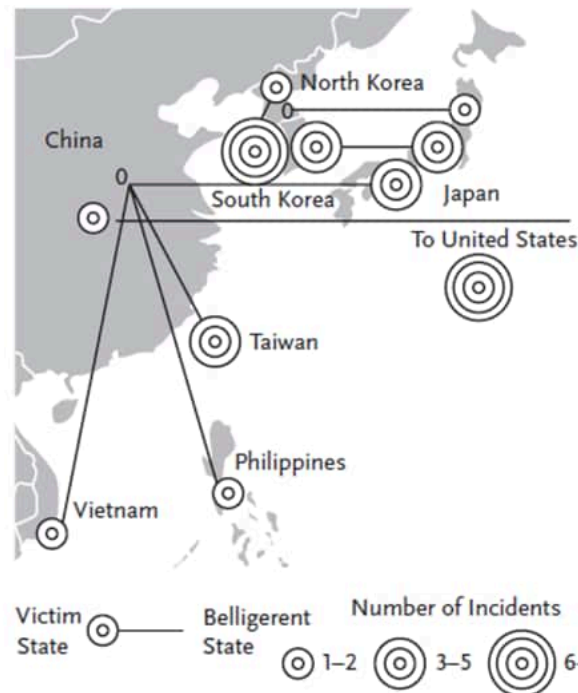
Georgia, July, 2008

- Paralyzed Georgia’s central bank and communications infrastructure and fifty-four government websites were disabled as Russian tanks rolled across its border in August 2008 (Kaplan, 2015).
- According to (Shakarian, 2011):
 - **First phase:** The Russian hackers and botnets launched DDoS attacks on government and media websites.
 - **Second phase:** They attacked financial institutions, businesses, educational institutions, Western media (BBC and CNN), and a Georgian hacker website.
 - “patriotic” Russian computer users were recruited through sites like “StopGeorgia.ru” which provided easy-to-use tools and instructions to launch DDoS from private machines. It even featured a user-friendly button called “FLOOD” which, when clicked, deployed multiple DDoS on Georgian targets.
- In **Georgian case, cyberattack and military operations** were conducted in **tandem** (Shakarian, 2011).

CYBER CONFLICTS NEAR TO HOME MIDDLE EAST, EAST ASIA & SOUTH ASIA



Cyber conflict in the Middle East.



- Triad of North Korea, South Korea and Japan show continued cyber conflict.
- Asian states of Japan, South Korea, Taiwan, and Vietnam have been the victim of **more cyber incidents than transnational terrorist attacks**.



India-Pakistan dyad features continued cyber conflict

(Valeriano and Maness, 2015).

NEPAL – INDIA RELATION

- November 2019: India's new political map places disputed territory of Kalapani inside its own borders. [TKP 2019]
- May 2020: India opened a road via Lipulekh, Nepal's territory. [TKP 2020]
- Nepal government unveiled a new political map in May 2020.

NATIONAL SECURITY

India's new political map places disputed territory of Kalapani inside its own borders

Nepal has long claimed Kalapani as part of its territory as per the Sugauli Treaty signed between Nepal and the then East India Company.



India's new political map (left) includes the disputed territory of Kalapani. Nepal's official map (right) Nepal's Survey Department

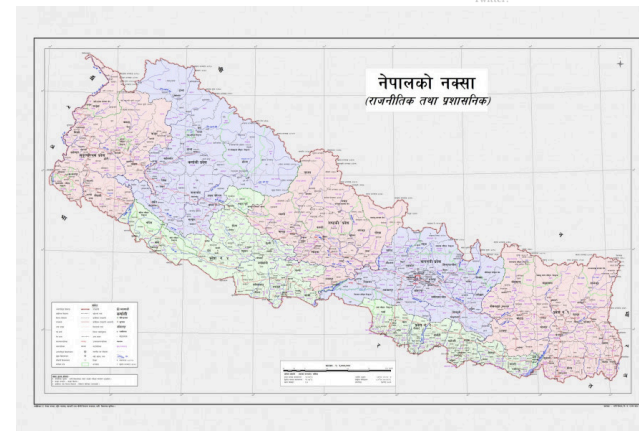


India opening a road via Lipulekh, a territory that Nepal claims, is a diplomatic failure

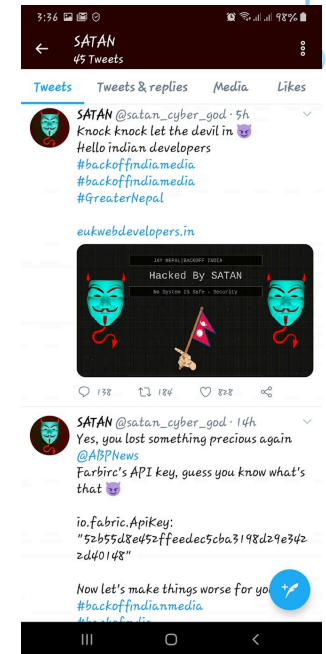
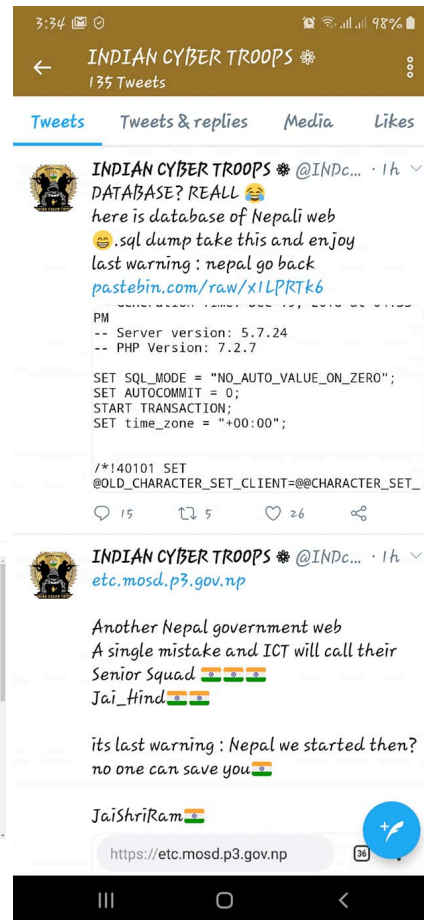
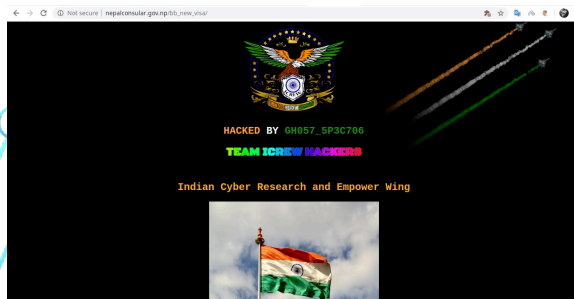
Despite the furore in Kathmandu over the inclusion of Kalapani on a new Indian map, the government has done little to reclaim lands that Nepal claims as its own.



India on Friday said it has inaugurated a link road from Darchula to Lipulekh. Photo via Indian Defense Ministry's Twitter.



CYBER ATTACKS BETWEEN NEPALI-INDIAN HACKERS



Such small-scale incidents are sporadic but growing! What if we face cyber threats like in Estonia and Georgia?

Report: Attackers Hacked Nepalese Bank's SWIFT Server

\$4.4 Million Moved to Accounts in US, UK and Japan via Fraudulent SWIFT Messages

Mathew J. Schwartz (@euroinfosec) • November 6, 2017

Twitter Facebook LinkedIn Credit Eligible

Get Permission



NIC Asia Bank advertisement celebrating this year's five-day Tihar - aka Diwali - Hindu festival, which is when hackers attacked the bank.

One of Nepal's largest private-sector commercial banks last month suffered a hack attack that led to attackers issuing fraudulent money transfers via the SWIFT interbank messaging service.

See Also: [Live Webinar | Enforcing Least Privilege Access in AWS Cloud Infrastructure with CIEM](#)

NIC Asia Bank, based in Kathmandu, said attackers initiated \$4.4 million in fraudulent money transfers from its accounts to accounts in six other countries, including the United States, the United Kingdom, Japan and Singapore, the [Himalayan News Service](#) reported Sunday.

Several diplomats in Delhi including those from Nepal on Pegasus list

Agency 2021-07-20 0

26 Shares



NEW DELHI, July 20: While reports of Indian politicians and journalists being targets of surveillance operations carried out with the help of Pegasus spyware took centre-stage on Monday, French newspaper Le Monde reported that several Delhi-based diplomats including those from Nepal were also on the list of potential targets for phone hacking from 2017-2021

नेपाल सरकार
गृह मन्त्रालय
नेपाल प्रहरी प्रधान कार्यालय
साइबर ब्यूरो

फोन: { ९८५१२८६७७०
०१-५३१९०४४
Ext: }
Email: cyberbureau@nepalpolice.gov.np
भोटाहिटी, काठमाडौं
मिति: २०७९-१२-२४ गते ।

प्रेस विज्ञप्ति

नेपाली सेनाको साइबर स्पेसमा हमला गर्ने व्यक्ति पक्राउ ।

नेपाली सेनाको साइबर स्पेसमा अनधिकृत पहुँच पुऱ्याउने उद्देश्यले विभिन्न समयमा साइबर हमला (Cyber Attack) भएको देखिन आएकोले आवश्यक अनुसन्धान तथा कारबाहीका लागि नेपाली सेनाबाट पत्र प्राप्त हुन आएको । साइबर हमलाको अनुसन्धान, प्राविधिक विश्लेषण तथा ह्युमन इन्टेलिजेन्सका आधारमा उक्त गैर कानुनी कार्यमा संलग्न जिल्ला स्याङ्जा, वालिङ्ग नगरपालिका वडा नं. १० घर भई हाल कास्की पोखरा महानगरपालिका वडा.न.१६ बाटुलेचौर डेरामा बसी घर धनीको ईन्टरनेट प्रयोग गर्ने वर्ष २१ को सागर ढकाललाई यस ब्यूरोबाट खटिई गएको टोलीले मिति २०७९/१२/२३ गते जिल्ला कास्की पोखरा महानगरपालिका वडा.न.१६, बाटुलेचौरबाटै पक्राउ गरी विद्युतीय कारोबार ऐन २०६३, अपराध अन्तर्गतको कसुरमा सम्मानित काठमाडौं जिल्ला अदालतको मिति २०७९/१२/२४ गतेको आदेशले दिन सात (७) म्याद थप भई आवश्यक अनुसन्धान कार्य भइरहेको ।

उप-निर्देशक
(पशुपति कुमार राय)
प्रहरी उपरीक्षक
प्रवक्ता एवं सूचना अधिकारी
सम्पर्क नम्बर: ९८५१२८६७७२

Hackers obstruct govt sites for four hours

By Himalayan News Service

Published: 09:45 am Jan 29, 2023



Hackers obstruct govt sites for four hours. File Photo: Reuters

KATHMANDU, JANUARY 28

Hundreds of government websites under the '.gov.np' domain, including the Office of the Prime Minister, the President's Office, and websites of all departments were hacked by people from unidentified places that obstructed accessibility to the websites from 12:00 noon to 4:00pm today.

CYBER ATTACKS IN NEPALI FINANCIAL INSTITUTIONS

VISA Cards fraud (ATM), मुद्दा संख्या – १४, माग दाबी लिइएको बिगो - ३,२१,६२,९३१/३०.

बैंकहरुबाट जारी भएका ATM /VISA कार्डहरुको Magnetic Stripe मा बैंकहरुबाट जारी भएको सक्कली DATA लाई मेटाई (Delete) गरी नक्कली DATA (ENCODE) गरी / राखी बैंकिङ कसुर गर्ने गरेको (use of Card reader, writer).

नक्कली (VISA) कार्डहरुको प्रयोग गरी समानहरु खरिद गर्ने कार्य (use of Card skimming set, Hidden Camera set)

कृषि विकास बैंक :- १७ वटा CBS system (T24) खातावालको उल्लेखित भनि आएको रकम रुपमा रेमिटेन्सको शाखाबाट नभएका लागु कृषि उपत्यकाका काठमाण्डौ गरी जारी चेक नाममा व्यक्तिहरुको विभिन्न तथा आफ्ना खातावालहरुले देखाई भएको जम्मा रकम खातामा कृषि रकम बढी भन्दा ३४ करोड.कुल रु लिई रकम मार्फत क्लियरिङ बैंकहरुबाट लगायतका.लि बैंक सिभिल र शाखाबाट का.लि बैंक बिकास हानिनोक्सानी लाई.लि बैंक बिकास

NIC Asia Bank:- SWIFT HACKING- विदेशी ह्याकरहरुले बैंकको कर्मचारीहरुको पासवर्ड कमप्रमाईज गरी रु ४६,५६,५०,५०५/- बराबरको रकम विदेशी बैंकहरुमा transfer गरेको ।

सनराइज बैंक :- सनराइज बैंक लिमिटेड बाट प्राप्त POS मेसिन बाट नक्कली कार्ड को माध्यमले अनाधिकृत रुपमा कारोबार गरिएको ।

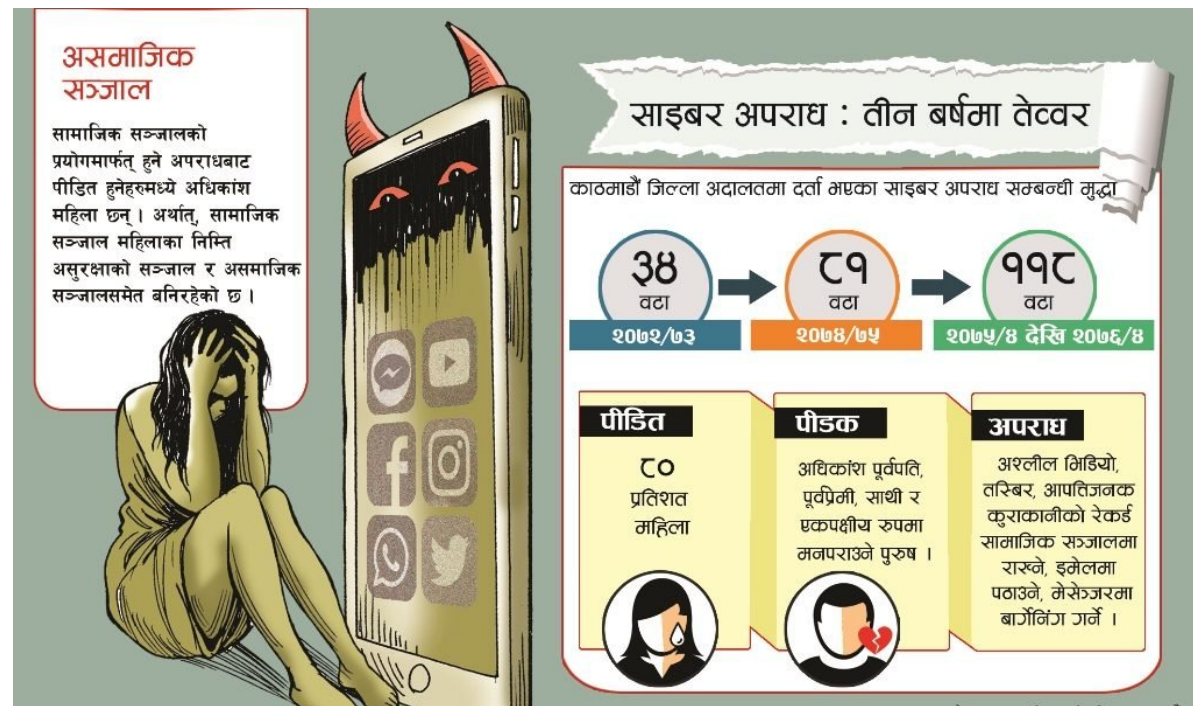
राष्ट्रिय बाणिज्य बैंक:- विशालबजार काठमाण्डौंमा USD खाता खोली ई-बैंकिङ, मोबाइल बैंकिङ र ई-सेवा वालेट जस्ता विधुतीय माध्यमको प्रयोग गरी आफ्नो USD खातामा अनाधिकृत रुपमा USD ७८,३८०/५० रकम जम्मा गरी भुक्तानी लिनको लागि ATM तथा PoS मेसिनहरु प्रयोग गरिएको ।

Source: CIB, 2022

RISE OF CYBER ATTACKS DURING CRISIS

Covid-19

- WHO [April 2020]
 - Fivefold increase in cyber attacks than last year directed at the Organization.



According to Nepal Police, six cybercrime incidents are reported everyday during Covid-19.

CYBER ATTACKS DURING CRISIS



EARTHQUAKE HAITI

Wall Info Events Photos Video Discussions

Write something...

Attach: Share

THIS IS SO GREAT!!! ALL THE HELP THAT IS IN HAITI AND ALL THE HELP THAT IS ON ITS WAY WOW MIRACLES DO HAPPEN GOD BLESS HAITI AND KEEP BLESSING THEM DAY BY DAY!!!!!!

23 minutes ago · Comment · Like · Report

UPDATE: PLEASE NOTE THAT AT 12 MIDNIGHT (PT) POSTING ON THIS SIGHT WILL BE HALTED UNTIL MY COUNTERPART IN FRANCE RELAUNCHES A FEW HOURS LATER. THIS IS OUR WAY OF SHOWING THE DEVILS THAT VIOLATED OUR SITE LAST NIGHT THAT GOD AND GOOD IS MORE POWERFUL THAN EVIL.

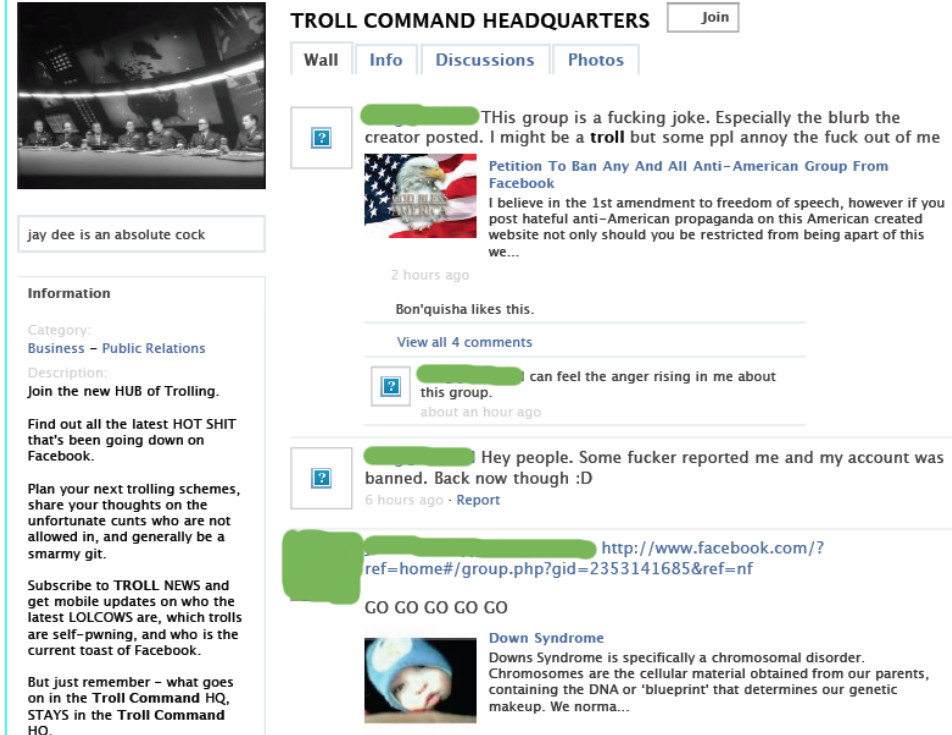
34 minutes ago · Comment · Like · Report

mosctha.org in

Haiti....
Help has arrived! Mosctha hit the ground and in two days we were able to aid over 300 wounded victims. A group of medical specialists and volunteers arrived in Haiti with a purpose to save lives. We were

Please post any information about missing people, the latest news and reliable NGOs in the groups Earthquake Haiti and Montreal pour Haiti. Thank you very much and please share this message with as many people as possible.

Immediately after the quake crisis responders were working together. Some citizens started groups on Facebook to coordinate disaster response.



TROLL COMMAND HEADQUARTERS

Wall Info Discussions Photos

Join

THIS group is a fucking joke. Especially the blurb the creator posted. I might be a troll but some ppl annoy the fuck out of me

Petition To Ban Any And All Anti-American Group From Facebook

I believe in the 1st amendment to freedom of speech, however if you post hateful anti-American propaganda on this American created website not only should you be restricted from being apart of this we...

2 hours ago

Bon'quisha likes this.

View all 4 comments

can feel the anger rising in me about this group.

about an hour ago

Hey people. Some fucker reported me and my account was banned. Back now though :D

6 hours ago · Report

<http://www.facebook.com/?ref=home#/group.php?gid=2353141685&ref=nf>

GO GO GO GO GO

Down Syndrome

Downs Syndrome is specifically a chromosomal disorder. Chromosomes are the cellular material obtained from our parents, containing the DNA or 'blueprint' that determines our genetic makeup. We norma...

As crisis responders were busy with response activities a Troll Command Headquarters was established. Group members used to jointly attack the crisis response groups on social media.

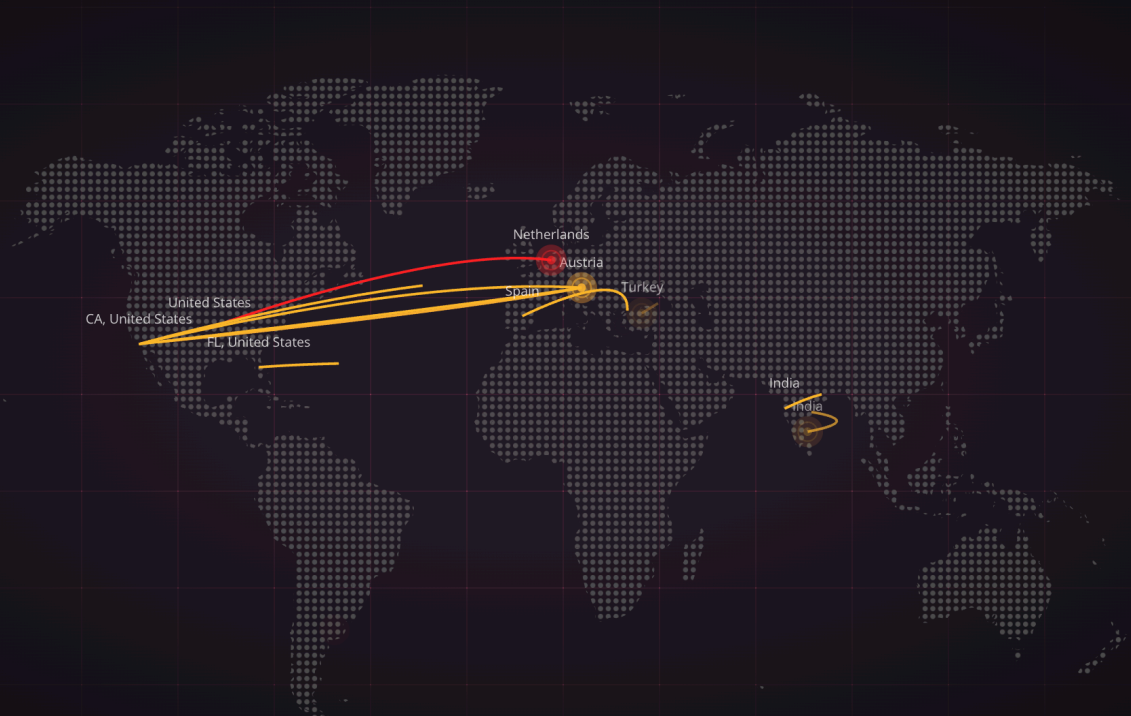


LIVE CYBER THREAT MAP

DON'T WAIT TO BE ATTACKED
PREVENTION STARTS **NOW >**

ATTACKS 🌐 Current rate - 4 +

- Web Client Enforcement Violation
13:18:07 FL, United States → India
- Web Server Enforcement Violation
13:18:07 India → India
- Web Client Enforcement Violation
13:18:07 CA, United States → Austria
- Web Client Enforcement Violation
13:18:07 Spain → Turkey
- Web Client Enforcement Violation
13:18:06 CA, United States → Austria
- dga-RouEt.TC.5ccfeWVL
13:18:06 United States → Netherlands



TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Mongolia
- Nepal
- Macao
- Georgia
- Kenya

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Education
- Healthcare
- Government

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Mobile
- Phishing
- Adware



- Malware
- Phishing
- Exploit

<https://threatmap.checkpoint.com/>

CHANGING PARADIGM IN CYBER THREATS

Malicious Acts

Hacking

Attacks

Cyber threats

Individual/Group

Disruptions

Damage

Individual/Group

State
Sponsored

Steal money, critical
info or espionage

State/Non-State

Info Warfare
Disinformation

Military Action

Interpol, July 2020

There has also been a “significant target shift” from individuals and small businesses to major corporations, governments and critical infrastructure

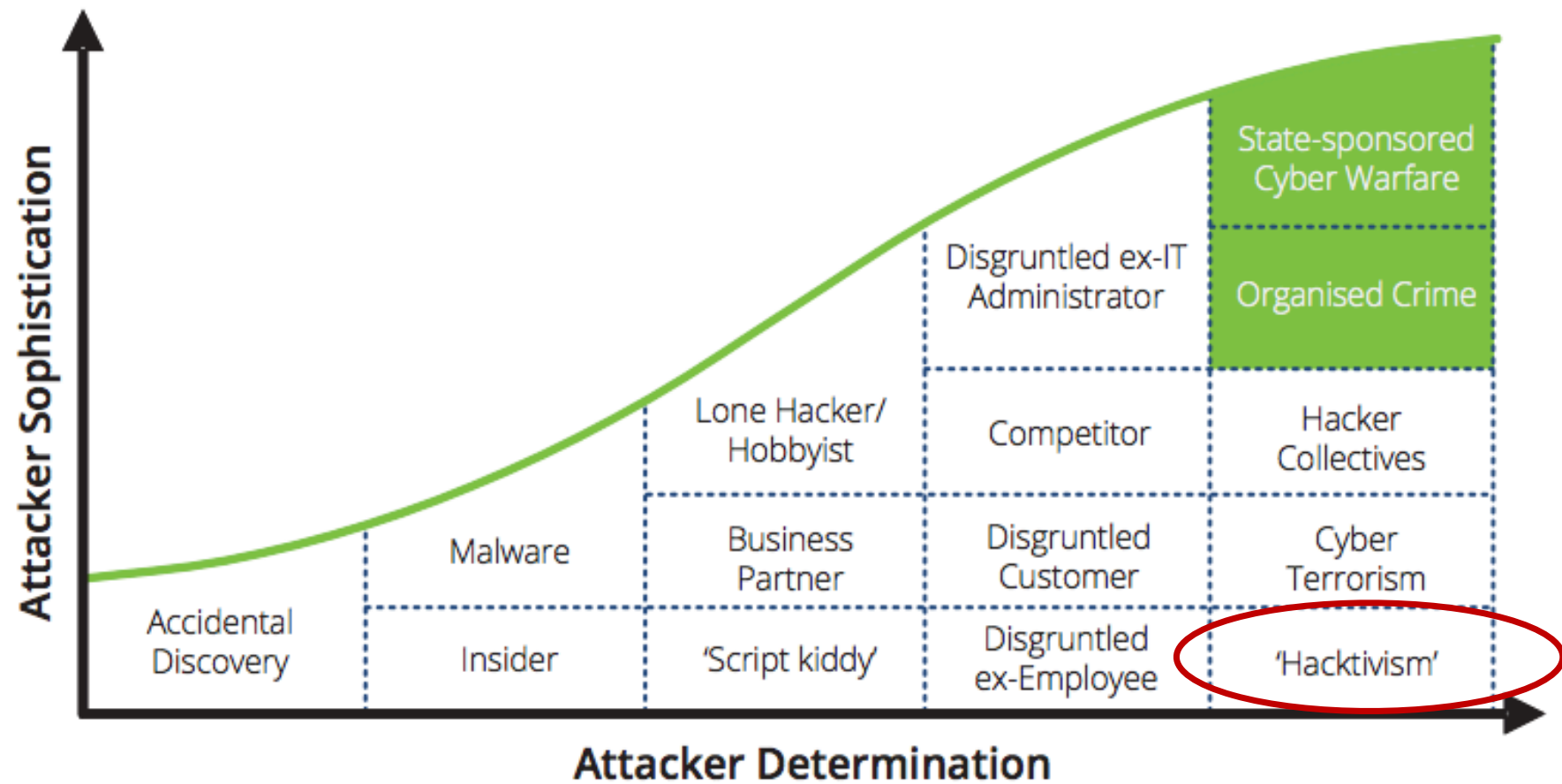


PHASES OF CYBER THREATS

	Realization (1980s)	Takeoff (1998-)	Mobilization (2003-)
Capabilities	US and few	Russia and many	China and everyone
Adversaries	Hackers	Hacktivists, Patriot Hackers, Virus and Worms	Neo-Hacktivists, Espionage, Malware
Major Incidents	Morris worm (1988): 1 st computer worm spread via the Internet	Moonlight Maze (1998): FBI inquiry into a cyber attack on United States GOVT NWs in 1998.	Estonia, Georgia STUXNET

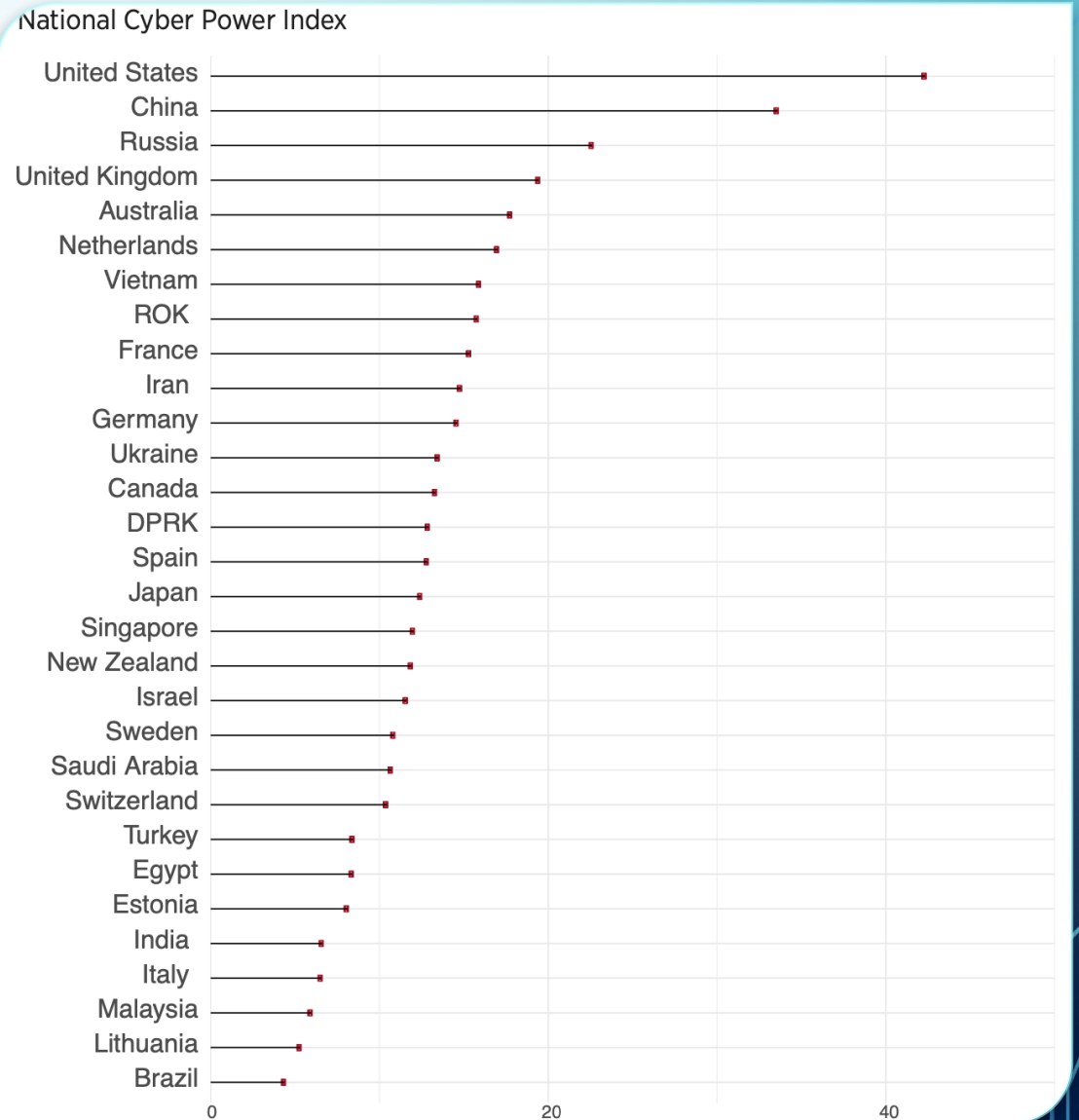
Source: Jason Healey, (2013) The Lessons of Cyber Conflict History, So Far..., Atlantic Council.

CYBER THREAT ACTORS



NATIONAL CYBER POWER INDEX

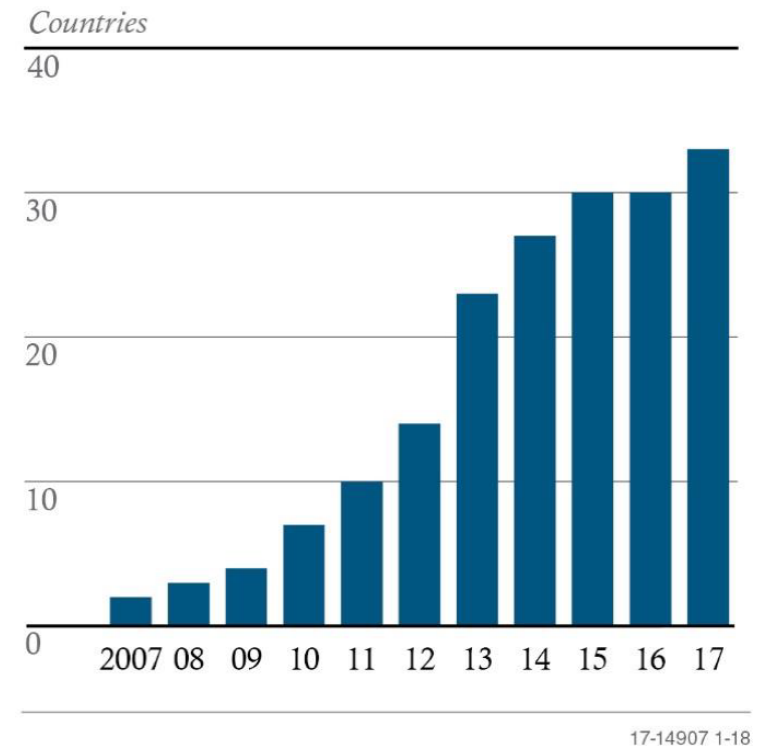
- Top 30 countries
- Source: **National Cyber Power Index 2022** by Julia Voo, Irfan Hemani and Daniel Cassidy, Belfer Center for Science and International Affairs, Harvard Kennedy School. 2023.



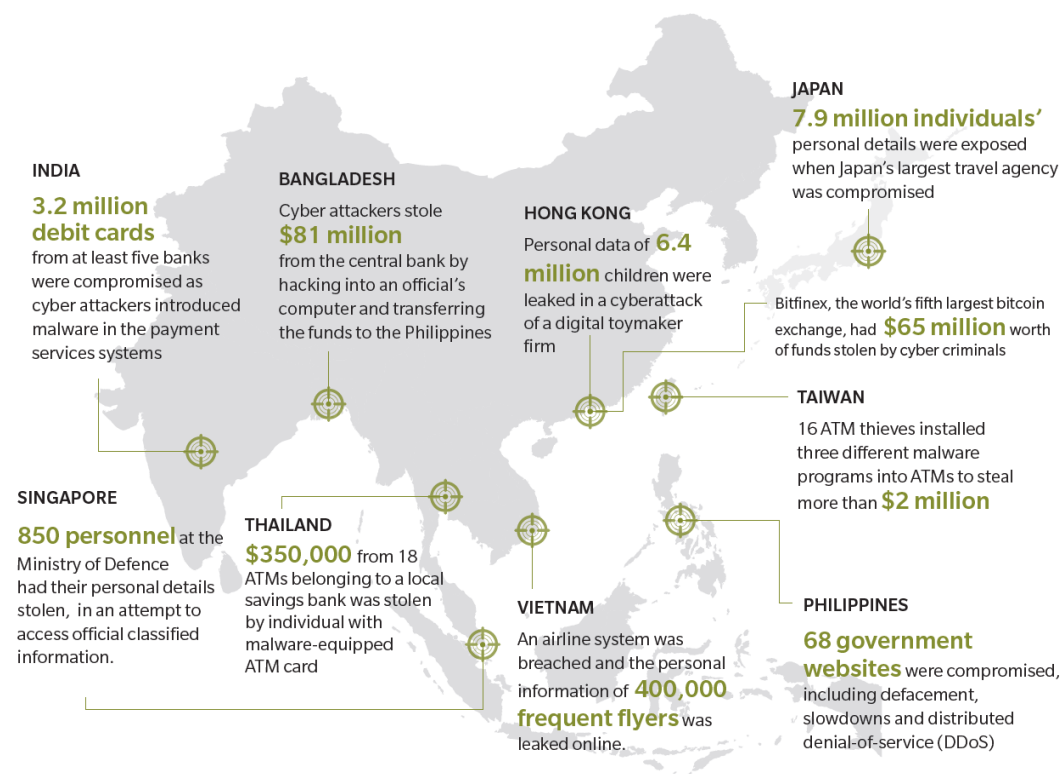
COUNTRIES WITH CYBER ATTACK CAPABILITIES

- Center for Strategic and International Studies (CSIS) report in 2011:
 - identified 33 states that include cyberwarfare in their military planning and organization. (10 from APAC)
 - **Cyberwarfare organizations:** Argentina, Brazil, Canada, China, the Democratic People's Republic of Korea, Denmark, Germany, India, Iran, the Republic of Korea, Switzerland and the United States and possible Cuba and Russian Federation.

Countries With Cyber Attack Capabilities



IMPLICATIONS OF RECENT INCIDENTS OF CYBER ATTACKS IN THE APAC REGION



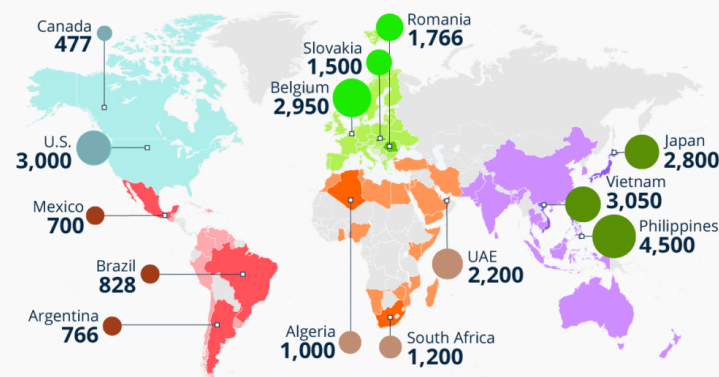
Cybercrime To Cost The World
\$10.5 Trillion
Annually By 2025

(Source: Cybercrime Magazine)

AI-FUELED FRAUD IS SURGING FAST

bright defense

TOP COUNTRIES BY REGION SHOWING THE SHARPEST RISE IN DEEPFAKE-RELATED FRAUD FROM 2022 TO 2023 (PERCENTAGE GROWTH)*



The report examines over 2 million identity fraud attempts across 224 countries and territories. All data has been aggregated and anonymized. *Regional classification based on the source.
Source: Sumsub Identity Fraud Report 2023

Break!



Strategy for Resilient Cybersecurity for Governance

Five Core Pillars



Identify & Govern

Asset inventory & risk framework



Protect

Controls & access management



Detect

Threat monitoring & analytics



Respond

Incident command & comms



Recover

Continuity & lessons learned

What the framework covers:

Governance Lifecycle — the five-stage policy cycle from design through to iterative review, ensuring cyber policy stays current with the threat environment.

Threat Landscape — the six highest-impact threat categories facing public sector organizations today, with relative risk ratings.

Maturity Ladder — a five-level progression model from ad hoc reactive posture to optimizing, intelligence-led defense — useful for self-assessment and roadmap planning.

Foundational Principles — the six architectural and cultural pillars (Zero Trust, Defense in Depth, Whole-of-Government coordination, Privacy by Design, Supply Chain Assurance, and Security Culture) that underpin the entire strategy

POLICY & GOVERNANCE LIFECYCLE



POLICY
DESIGN



STAKEHOLDER
ALIGNMENT



IMPLEMENTATION



AUDIT &
COMPLIANCE



REVIEW &
ITERATE

Governance Lifecycle — the five-stage policy cycle from design through to iterative review, ensuring cyber policy stays current with the threat environment.

PUBLIC SECTOR THREAT LANDSCAPE



Ransomware on Critical Infrastructure

Risk level



Nation-State Espionage

Risk level



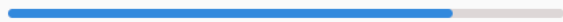
Insider Threats & Credential Abuse

Risk level



Supply Chain Compromises

Risk level



Phishing & Social Engineering

Risk level



Data Exfiltration & Privacy Breaches

Risk level



Threat Landscape — the six highest-impact threat categories facing public sector organizations today, with relative risk ratings.

CYBERSECURITY MATURITY LADDER

1 INITIAL	Ad hoc, reactive. No formal policies; incidents handled informally case-by-case.	
2 DEVELOPING	Basic controls exist. Policies documented but inconsistently applied; partial asset visibility.	
3 DEFINED	Standardised & trained. Org-wide framework; SOC operational; regular audits and drills.	
4 MANAGED	Measured & risk-driven.	KPIs tracked; threat intelligence integrated; continuous monitoring active.
5 OPTIMISING	Adaptive & intelligence-led.	AI-assisted detection; cross-agency intel sharing; proactive threat hunting.

Maturity Ladder — a five-level progression model from ad hoc reactive posture to optimizing, intelligence-led defense — useful for self-assessment and roadmap planning.

FOUNDATIONAL PRINCIPLES



Zero Trust Architecture

Never trust, always verify — every user, device, and network connection continuously authenticated.



Defence in Depth

Multiple overlapping security layers so no single control failure leads to full compromise.



Whole-of-Government

Unified cyber policies, shared services, and central coordination across all public entities.



Privacy by Design

Citizen data protection embedded from the outset, not retrofitted — GDPR & sovereignty compliant.



Supply Chain Assurance

Vendor risk management, software bill of materials (SBOM), and procurement security standards.



Security Culture

Mandatory awareness training, tabletop exercises, and executive-level cyber literacy programmes.

Foundational Principles — the six architectural and cultural pillars (Zero Trust, Defense in Depth, Whole-of-Government coordination, Privacy by Design, Supply Chain Assurance, and Security Culture) that underpin the entire strategy

CYBERSECURITY ROADMAP FOR NEPAL



Legal & Policy: Cyber Act, Policy, Data Protection



Institutional: CERT, CyberBureau, NA CyComnd



Infrastructure: Power, Banking, Telecom



Workforce: Curriculum, Scholarships, Reserve



Global: CERT-In, APCERT, ITU



E-Gov: Databases, Pen Test, ISO



Finance: NRB, SWIFT, MoFA



Awareness: Phishing, Campaigns



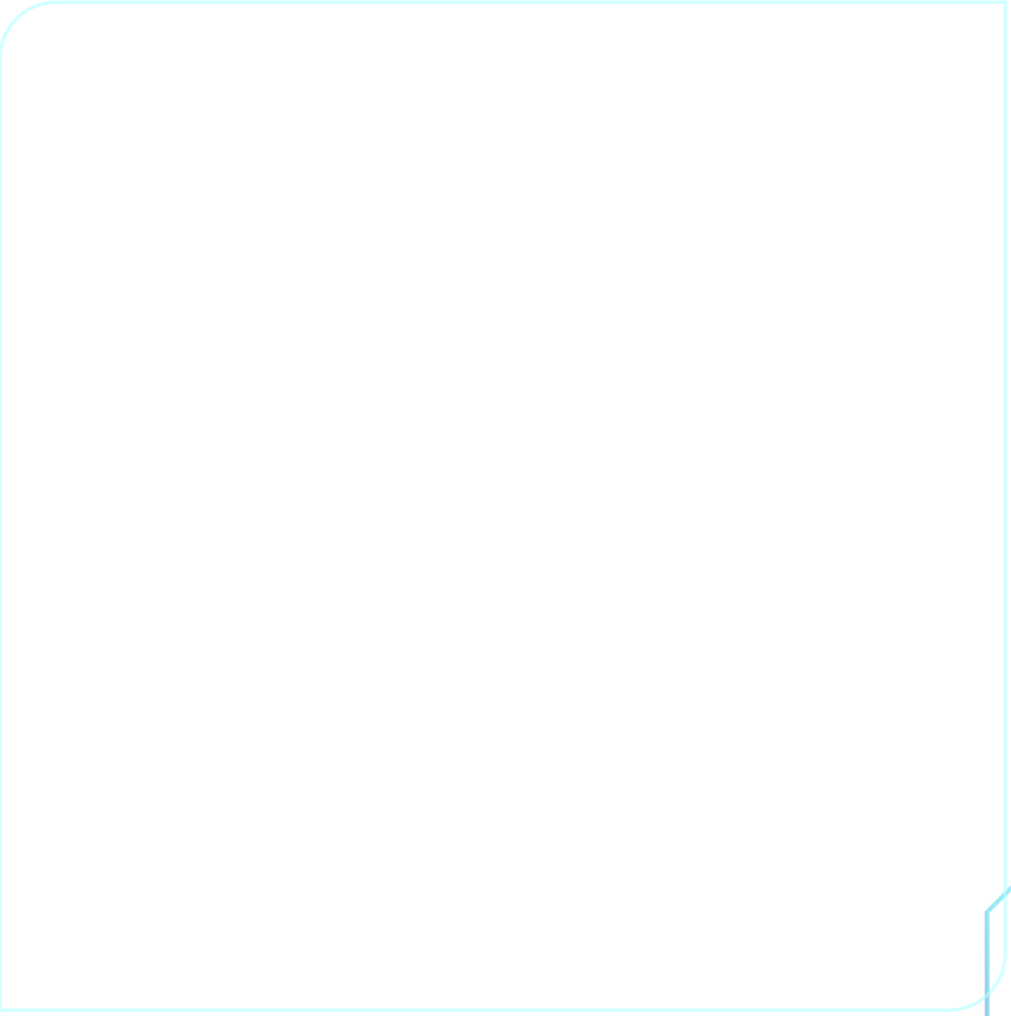
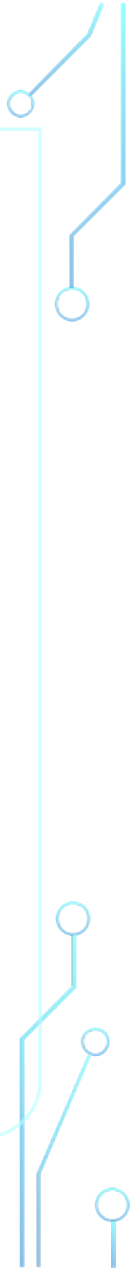
Geopolitics: Balance, Audit



Priority: Law → Infra → Skills → Global



POLICY FRAMEWORKS

- Constitution of Nepal
 - National Security Council Policy 2073
 - Telecom Act 2053
 - Cybersecurity Bylaws (NTA) 2077
 - Cyber Security Policy (MOCIT) 2078
 - Privacy Act 2075
 - Foreign Policy 2076
 - National Health Policy 2076
 - IT Guidelines (NRB) 2069
 - Radio Act 1957
 - Cybersecurity Policy 2080
 - IT and Cybersecurity Bill
- 
- 

RECOMMENDATIONS

National Policy Framework (Cyber Security @ National Level)

IT and Cyber Security Bill 2080
Cyber Security Policy – 2016 (Need to update and pass it)
National Security Council Act must include Cyber Defense

Cyber Security Command Center

Cyber Defense Command Center – NA
National Computer Emergency Response Team (CERT) - Nep CERT

Cybersecurity Intelligence Mechanism

Sharing of information between stakeholders and organizations/businesses

Strengthen Cyber Crime Investigation

Cyber Bureau of Nepal Police
Digital Forensic Labs
Cyber Command at NA

RECOMMENDATIONS



More investment on

Security of critical infrastructures, DBs and networks

Capacity Building of ICT HR on new and emerging technologies



Mandatory ICT System Audit of Gov & non-Gov ICT Systems

E.g. Nepal Rastra Bank and commercial banks



Focus on cognitive-human aspect, social engineering



Cyber Security Research

POLICY RECOMMENDATIONS

साइबर सुरक्षा भनेको कम्प्युटर सुरक्षा मात्र नभई एक विस्तृत राष्ट्रिय सुरक्षाको विषय हो । किन भने सूचना तथा संचारप्रविधि प्रयोग नहुने कुनै पनि क्षेत्र छैन । तसर्थ नेपालका विभिन्न राष्ट्रिय नीति, ऐन, नियमावली, निर्देशिकाहरूलाई बदलिंदो साइबर परिस्थिति अनुसार परिमार्जन गरी राष्ट्रिय साइबर सुरक्षा नीतिसँग आबद्ध गर्नुपर्दछ ।

- राष्ट्रिय सुरक्षा नीति २०७३ लाई परिमार्जन गरी बुँदा १.९ र २.८ मा उल्लिखित साइबर अपराध र विद्युतीय वित्तीय संरचना सुरक्षा सहित साइबर डिफेन्स तथा महत्वपूर्ण सूचना प्रणाली (क्रिटिकल पूर्वाधार) जस्तै सूचना तथा संचार, स्वास्थ्य, शिक्षा आदिलाई समेत सुरक्षा प्रदान गर्ने व्यवस्था थप गर्ने ।
- दूरसंचार तथा इन्टरनेट सेवा प्रदायकहरूको महत्वपूर्ण सूचना प्रणाली (क्रिटिकल पूर्वाधार) सुरक्षाका लागि दूरसंचार ऐन २०५३ ले व्यवस्था गरे अनुरूप नेपाल दूरसंचार प्राधिकरणले तयार गरेको साइबर सुरक्षा विनियमावली २०७७ लाई राष्ट्रिय साइबर सुरक्षा नीतिले आकर्षित गर्न सक्ने व्यवस्था गर्ने । यस विनियमावलीले नसमेट्ने क्षेत्रको हकमा साइबर सुरक्षा नीतिमा उल्लेख गर्ने ।
- तथ्याङ्क सम्बन्धी गोपनीयता तथा सङ्कलित सूचनाको संरक्षणको व्यवस्था गरिएको वैयक्तिक गोपनीयता सम्बन्धी ऐन २०७५ को परिच्छेद ६ र परिच्छेद १० र बुँदा २५ लाई साइबर सुरक्षा नीतिले आकर्षित गर्न सक्ने व्यवस्था गर्ने ।
- परराष्ट्र नीति २०७६ मा उल्लिखित साइबर अपराध मात्र रहेको हुनाले साइबर जोखिम तथा साइबर डिफेन्स समेत थप गर्ने । साथै सिमानाको परिभाषा परिमार्जन हुँदै गएको अवस्थामा परराष्ट्र नीतिमा नेपालको भूमि अरु राष्ट्रको विरुद्धमा मात्र होइन साइबर पूर्वाधारहरू समेत प्रयोग गर्न दिइने छैन भन्ने प्रतिबद्धता थप गर्नुपर्ने ।
- राष्ट्रिय स्वास्थ्य नीति २०७६ को बुँदा ६.१५ लाई परिमार्जन गरी साइबर सुरक्षा कार्यनीति निश्चित गर्ने प्रावधान थप गर्ने ।
- नेपालका बैंकहरूका लागि राष्ट्र बैंकले जारी गरेको सूचनाप्रविधि निर्देशिका २०१२ (२०६९) लाई परिमार्जन गरी कुनै पनि वित्तीय कारोबार गर्ने संस्थाहरूले अनिवार्य सूचना प्रणाली अडिट गर्नुपर्ने प्रावधान थप गर्ने ।
- रेडियो सिग्नल सूचना सुरक्षार्थ रेडियो ऐनलाई साइबर सुरक्षा नीतिले आकर्षण गर्न सक्ने प्रावधान राख्ने ।

विचारः

राष्ट्रिय सुरक्षाका लागि साइबर सुरक्षा



डा. राजीव सुब्बा २०७८ जेठ २६ गते ९:०८ मा प्रकाशित

5 प्रतिक्रिया

429 Shares

f

X

WhatsApp

Telegram



सूचना तथा संचारप्रविधिको विकाससँगै मानव सभ्यताले ठूलो फड्को मारेको छ । महीनौं लगाएर पुग्ने चिठ्ठी इमेल मार्फत तुरुन्तै पुग्छ । शहरमा बस्ने डाक्टरले 'टेली मेडिसिन' मार्फत दुर्गमका बासिन्दाको स्वास्थ्य परीक्षण गर्न सक्छन् । ताप्लेजुडका कृषकहरूले संसारभरि 'इ-कमर्स' मार्फत आफ्नो उत्पादन बेच्न सक्छन् । सुर्खेतमा पढ्ने छोरीको स्कूल शुल्क हुम्लामा बस्ने आमाको मोबाइल मार्फत सजिलै तिर्न सकिन्छन् ।



राष्ट्रिय सुरक्षाका लागि साइबर रक्षा प्रणाली अनिवार्य छःडा.राजिब सुब्बा डिआइजी II Dr.Rajib Subba Views.



Kendrabindu News 793K subscribers

Subscribe

30

Share

Clip

Save

...

965 views Feb 25, 2020

राष्ट्रिय सुरक्षाका लागि साइबर रक्षा प्रणाली अनिवार्य छःडा.राजिब सुब्बा डिआइजी, नेपाल प्रहरी | Dr.Rajib Subba Views.

यो साइबर वारको समय हो -राजीव सुब्बा, डिआइजी, नेपाल प्रहरी | Cyberwar-Rajeev Subba

तेस्रो विश्व युद्धको पटक-पटक चर्चा हुने गरेको छ । धेरै राष्ट्रले आणविक होडबाजी समेत गरिरहेका छन् । तर युद्ध विज्ञहरू भन्छन् - 'अबको युद्ध बन्दुक वा आणविक अस्त्रले लडिदैन ।' उनीहरूका अनुसार अबको युग साइबरको हो । त्यसकारण साइबरको प्रयोग गरेर नै अबको युद्ध हुन्छ । विश्वयुद्ध भयो भनेपनि साइबर मार्फत नै लडिन्छ । यसै सन्दर्भमा केन्द्रबिन्दु न्यूज (युट्युव) च्यानलमा नेपाल प्रहरीका डिआइजी राजीव सुब्बाले आफ्नो धारणा राखेका छन् । उनको यो विश्लेषणत्मक भनाईलाई केन्द्रबिन्दुले भिडियो आर्टिकल भनेको छ । हेर्नुहोस् भिडियोमा :

CONCLUSIONS

- Recent incidents indicate that historical conflicts, critical infrastructure and cyberattacks are all interrelated (Karatzogianni, 2008).
- All conflict from now on will have some degree of cyberspace flavor (Demchak, 2012).
- Cyberspace can't be treated as a separate arena. It must be integrated into all elements of national power (Grant Schneider, 2018).
- Moreover, the use of **citizen hackers and other non-state parties** are changing the traditional warfare (White, 2018).
- Nepal's geo-location is unique and strategic.
- Geo-politics: Two giant neighbors have cyberwarfare capabilities.
- Bottom line is cyber threats are growing and security and critical infrastructures become more vulnerable when a crisis arises!
- We all should work together to make more cyber resilient Nepal.

MAJOR REFERENCES

- Kello, L. (2017). *The Virtual Weapon and International Order*. New Heaven, London: Yale University Press.
- Kaplan F. (2016) *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster
- Valeriano, B., & Maness, R. C., (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press: New York.
- Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. New York: Broadway Books.
- Kozlowski, A., (2014). Comparative Analysis of Cyberattacks on Estonia, Georgia, and Krygyzstan. *European Scientific Journal* February, Special Edition, vol.3, ISSN: 1857 – 7881.
- Chen, T. M. (2014), *Cyberterrorism After STUXNET*. Published by: Strategic Studies Institute, US Army War College (Jun. 1).
- James L. (2013). *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia*, Prepared for the Lowy Institute MacArthur Asia Security Project, CSIS. Last accessed on 10/30/2017 at https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130307_cyber_Lowy.pdf
- Loukas, Gan and Vuong. (2013). A Review of Cyber Threats and Defence Approaches in Emergency Management. *Future Internet*, 5(2), 205-236, doi:10.3390/fi5020205.
- Reveron, D. S. (2012). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington/DC: Georgetown University Press.
- Karatzogianni, A. (Eds.). (2008). *Cyber-Conflict and Global Politics*, London, UK: Routledge.
- Scott, W.R. (2001). *Institutions and organizations*. Thousand Oaks, California: Sage.



QA

It takes a village
to manage
cybersecurity
risk.

THANK YOU