Indian Cyber Resilience: Based on the Indian Dutch Cyber Security School 2020 Students' Gamified Assessment

As part of the 2020 Indian Dutch Cyber Security School (IDCSS), students had the opportunity to play the Indian Cyber Resilience Game. IDCSS is an online cybersecurity school addressed to Indian and Dutch higher education students and young professionals. The school included lectures and assignments, also known as challenges, on the most trending topics regarding cybersecurity.

The intent of the game was to further educate the students on all different aspects of cyber resilience and challenge them to assess what capabilities are required to make India more cyber resilient. The game was played over a period of five days by more than 200 students. Here, the results of the game are put in the broader perspective of the ambitions and programs India is implementing. These will in turn be related to the Sustainable Development Goals. But first, we will elaborate on the *Digital India* program and the array of cyber threats India currently faces. After this, we will present and explain the results of the game. Finally, we will make some general observations on the results of the game.

The government of India has been working on the *Digital India* program.[i] The aim of this ambitious program is to "transform India into a digitally empowered society and knowledge economy". More specifically, *Digital India* seeks to alleviate the shortcomings of national e-governance initiatives in the 1990s, such as the "lack of integration amongst government applications and databases, low degree of government process re-engineering and lack of scope for leveraging emerging technologies like mobile and cloud". The program focusses on digital infrastructure as a core utility to every citizen, governance & services on demand, and digital empowerment of citizens.[ii] There are nine pillars in total that form the basis of the Digital Indian program, which stand independently and together form a comprehensive vision that applies to the totality of governmental ministries and departments:[iii]

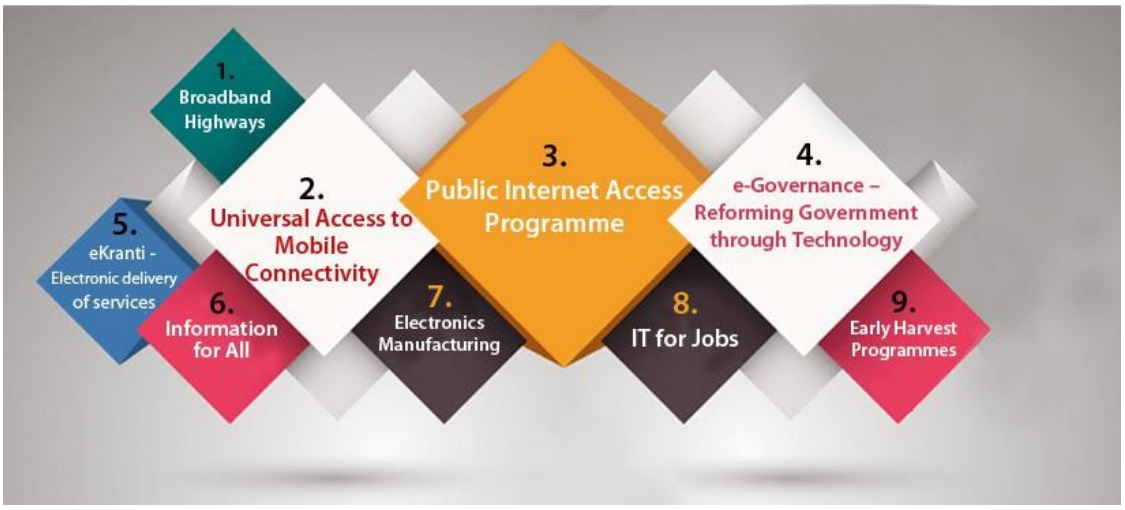

Figure 1 How Digital India will be realized: Pillars of Digital India

These pillars are both new and existing ones that got revised to fit into the digital environment of today.

To implement the *Digital India* program, Indian policymakers must collaborate with individual states to fulfil the goals of policies on e-governance with the aim of promoting citizen-centric services, accessibility to ICT infrastructure, and interoperability of applications.[iv] To be implemented, coordination between the government's ministries and departments with the states is not sufficient. The government should also consult with industry and civil society to create the right conditions for innovation. When consulting with the industry, the government may further form public private partnerships to monitor private actors when implementing its policies.

Prime Minister of India, Shri Narenda Modi, iterated during his speech at the UN General Assembly on September 2015 that "Today, much of India's development agenda is mirrored in the Sustainable Development Goals".[v] In particular, certain Indian initiatives under the *Digital India* program directly reflect UN Sustainable Development Goals (SDGs).[vi]

Figure 2 Sustainable Development Goals

Examples of these include:

Aadhaar: Aadhaar Identity Platform serves to provide every citizen with a unique identification number, to remove the risk of duplicate or fake identities and give citizens more direct access to governmental and state services. The enrolment to the database is voluntary and is concluded through the intake of certain demographic and biometric information.[vii] The Aadhaar Identity Platform addresses the SDGs of Good Health & Wellbeing (No. 3), Quality Education (No. 4), Gender Equality (No. 5), Decent Work & Economic Growth (No. 8), and Reduced Inequalities (No. 10).

MyGOV: MyGov is an online participatory platform that enable citizens' interaction with the government. Through the platform, people can engage in discussions, tasks, talks, polls and blogs on various groups and on various topics covering a wide range of activities of the Indian society, like agriculture, communications and education.[viii] The platform satisfies the SDGs of Peace, Justice & Strong Institutions (No. 16) and Partnerships for the Goals (No. 17) by managing to bring individuals, civil society and industry in an online forum to exchange views on public policy issues and actively participate in Indian governance.

Common Service Centers: Common Service Centers are behind the digitization initiatives that are promoted through *Digital India*. They are physical centers in rural and remote areas of India where access to electronic systems, such as computers, and the Internet is not always feasible. Therefore, citizens can enjoy public utility services, social welfare schemes, healthcare, financial, education and agriculture service.[ix] This structure corresponds to the SDGs of Affordable & Clean Energy (No. 7), Decent Work & Economic Growth (No. 8), Industry, Innovation & Infrastructure (No. 9), Sustainable Cities & Communities (No. 11), and Responsible Consumption & Production (No. 12). More specifically, common service centers seek to promote access to information for citizens of remote and rural areas, quality education, especially in relation to digital skills, quality health services and, upgrade rural communities through the adoption of innovative ideas.

Mission on Agriculture and Public Distribution System: The aim of the Mission is to address food insecurity in India by creating the Agricultural Knowledge System and integrating agricultural knowledge services with *Digital India*-infrastructure. The Mission takes place in the wider context of Digital India and brings together policymakers, investors, and farmers.[x] The Mission satisfies the SDGs of No Poverty (No. 1), Zero Hunger (No. 2), Clean Water and Sanitation (No. 6), Climate Action (No. 13), Life Below Water (No. 14), and Life on Land (No. 15) by ensuring access to information and knowledge and thus enabling the work of farmers on a day-to-day basis.

Cyber-vulnerabilities in India

In 2018, India was one of the top three countries with the most cyber-attacks in the world and second in terms of cyber targeted attacks.[xi] The latter form of attacks are mostly state-sponsored attacks with the aim of accessing intelligence, disrupting internet infrastructure, sabotaging government services, and interrupting the financial system. An example of this is the India-Pakistan case, where Pakistani hackers targeted India's telecommunication and national research institutes to gather intelligence on governmental officials and their activities. [xii]

Regarding cyber-attacks, the most often observed cyberthreats in India are cryptocurrency mining, malware, ransomware, drive by downloads, and data breaches.[xiii] Data on malware and ransomware attacks reveal that India has one of the highest rates of attacks in the Asia-Pacific.

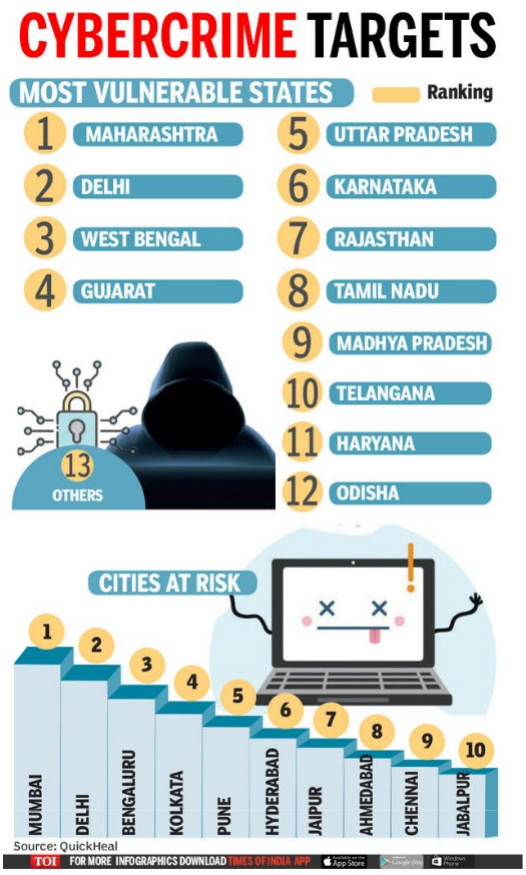

Figure 3 Mumbai at topmost risk of cyber-attack, May 21, 2019 India Times

Results of the student's assessment

Students participating in the IDCSS2020 were asked to assess the capabilities India requires to enhance its cyber resilience using a game. In total, some 200+ students with technical, policy and legal backgrounds took part in the exercise. The National Cyber Resilience Game is a game in line with the 'Serious Gaming'-concept. The main purpose of the game is to increase awareness on relevant capabilities and capacities that are needed to increase cyber resilience; to address what cyber resilience means for the planning of policies, activities, and operations of different ministries; and what role various relevant actors can or should play. Moreover, the game also offers the students the opportunity to learn more about and get familiar with the wide range of capabilities countries have in their 'toolbox' to strengthen their cyber resilience.

At the centre of the game is the playing board, consisting of two axes which represent the solution space players must explore in response to the challenge at hand – in this case, making India more cyber resilient. Simply put, the playing board represents the solution space, while the capabilities are the potential solutions which can be applied by the students.

As mentioned, the playing board has two axes. The horizontal axis represents the strategic function (threat mitigation, prevention, deterrence, etc.) of a certain capability, while the vertical axis represents the strategic sector (military, economic, etc.). Whenever placing a capability, students need to identify in which strategic sector it falls and what strategic function it has. This determines where the capability will be placed on the playing board.

The definition of a capability is "the ability to do something in order to establish an intended effect". An example of a capability would be: *The ability to trace and halt cyber attacks through military (intelligence) operations in order to reduce their disruptive consequences and facilitate legal proceedings.*

Game Results

So, which capabilities did the students deem important or necessary to make India more cyber resilient? When analysing the game results, a few things stand out.

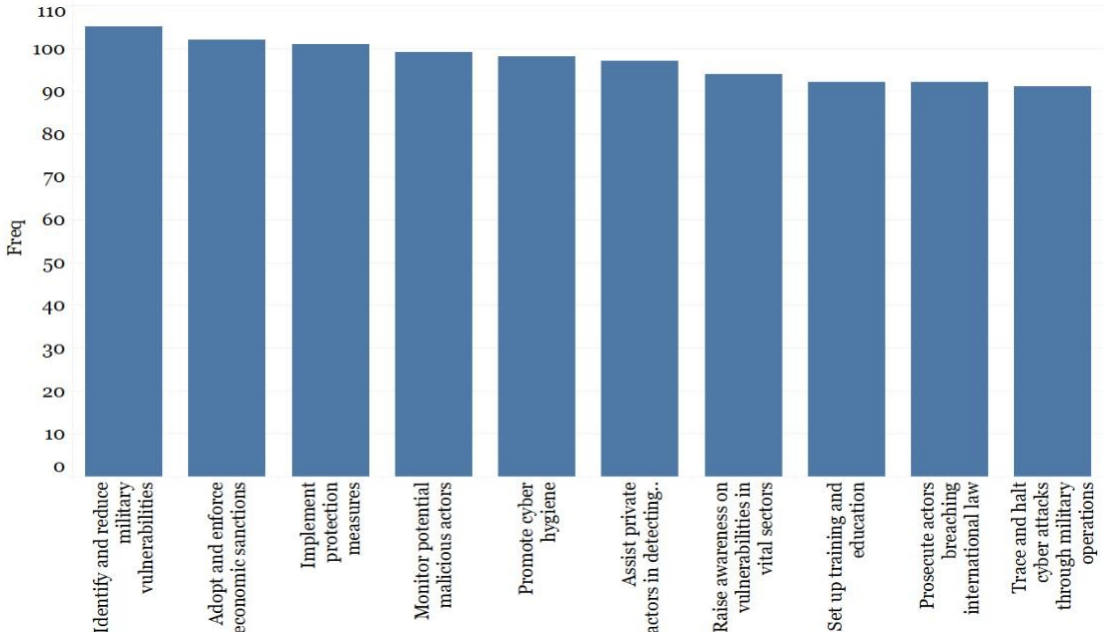

Figure 4: Top 10 Capabilities

The capability that was placed most often is *Identify and reduce military vulnerabilities* (104 times). The majority of students who applied this capability determined that it has the function of preventing cyber-attacks and protecting against cyber-attacks. The reason many of the students prioritized this card potentially has to do with the fact that military vulnerabilities can be exploited to a great extent and could have major consequences for national security. Therefore, it would be pivotal for them to be identified and reduced. As one of the students put it: "military information is sensitive and needs to be protected at all costs since it compromises the nation's security when leaked. This strict action will strongly discourage such attempts."

The other most often placed capabilities were:

Capability	Times placed	Most often placed Sector	Most placed Function
Adopt and enforce economic sanctions	104	Economic	Protection & prevention
Implement protection measures	101	(Counter)intelligence	Protection & prevention
Monitor Potential malicious actors	99	(Counter)intelligence	Protection & prevention
Promote cyber hygiene	98	Economic	Mitigation
Assist private actors in detecting cyber-crimes and -attacks	97	Public-private partnership	Protection & prevention
Raise awareness on vulnerabilities in vital sectors	93	Public-private partnership	Protection & prevention

Set up training and education	92	Public-private partnership	Mitigation
Prosecute actors breaching international law	92	Law Enforcement	Deterrence
Trace and halt cyber-attacks through military operations	91	Military	Response

Table 1 The most often played capabilities

The ten most often placed capabilities are from different sectors and have different functions, as seen be seen in Table 1. Interestingly enough, none of the top ten capabilities belong to the sector 'Diplomacy', which suggests that the students did not deem traditional diplomatic tools to have priority in order to make India more cyber resilient. Capabilities from the public-private partnership sector, however, were placed more often - which shows that the students believe capabilities resulting from cooperation between public and private actors are of importance. Additionally, the students seem to place an emphasis on capabilities that prevent cyber-attacks and -threats rather than capabilities which respond to them.[1]

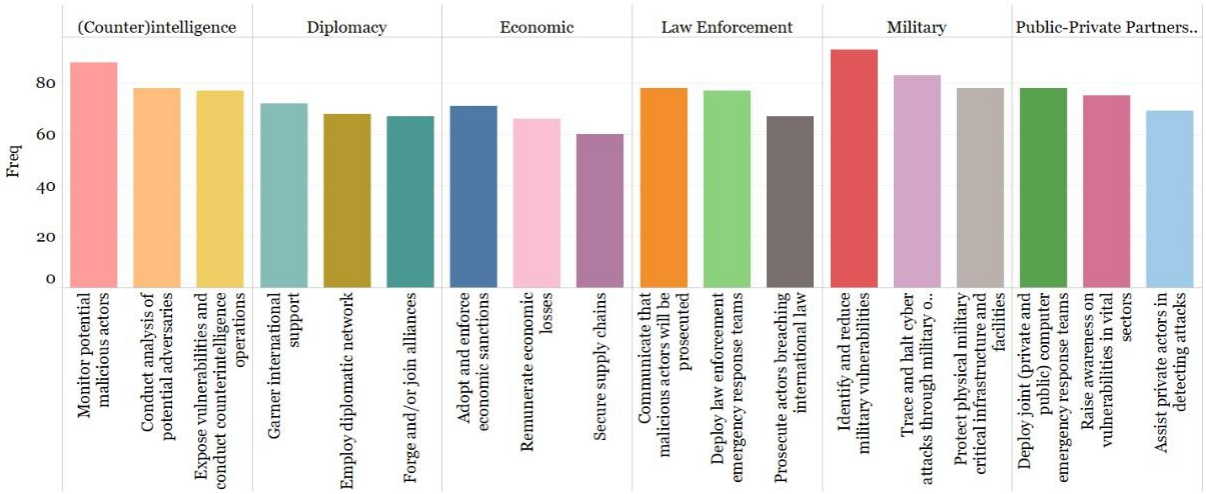

Figure 5: Top 3 Capabilities per Strategic Sector

Figure 5: Top 3 Capabilities per Strategic Sector portrays the top three most often placed cards per strategic sector. The students applied a wide range of capabilities from different strategic sectors. Within these sectors however, students showed to prefer certain capabilities. In the (counter)intelligence sector for instance, students placed a heavy emphasis on monitoring and identifying potential malicious actors. Regarding diplomacy, garnering international support was prioritized, while the capability of adopting and enforcing sanctions was deemed the most important 'tool' from the economic 'toolbox'. When looking at the most often applied capabilities from the law enforcement sector, it stands out that both the capabilities of (1) communicating that malicious actors will be prosecuted and (2) following through with this by prosecuting actors breaching international law were often applied by the students. This suggests that students are of the opinion that communicating thresholds and enforcing these should play a significant role.

1 An important sidenote here is that the number of 'placements' as shown in the table only represents how often the capability was placed. Where on the board this specific capability was placed may differ – the sector and functions shown in the table represent the most often picked position of that specific capability.

Finally, students also applied capabilities from the Public-Private Partnership sector, thereby communicating that cooperation between the government and private actors is necessary to make India more cyber resilient. The top three within the Public-Private Partnership sector, however, also shows that they placed an emphasis on top-down cooperation – the government supporting the private sector.

Observations

The student's collective brainpower was used to make an estimate of what India should pay attention to, with regards to cyber resilience, when implementing its digitization programmes. India is going through a period of immense change while digitalizing many of its functions. Irrespectively of what measures will be undertaken to make India more cyber resilient, the respective *attack surfaces* will grow, which in practice means that making India cyber resilience is not a one-off activity. It will require a constant and further enhanced effort because many of its core functions, especially in critical infrastructures such as financial systems, e-government applications and Aadhaar, will make India more effective and efficient on the one hand, but at the same time will potentially make India more vulnerable to cyber threats if they are not implemented cyber secure enough.

We hope that the students appreciated the game and learned a lot about the many aspects regarding national cyber resilience.

Endnotes

---

i Ministry of Electronics & Information Technology. "Introduction | Digital India Programme," n.d. https://www.digitalindia.gov.in/content/introduction.

ii Ministry of Electronics & Information Technology. "Vision and Vision Areas | Digital India Programme," n.d. https://digitalindia.gov.in/content/vision-and-vision-areas.

iii Ministry of Electronics & Information Technology, "Programme Pillars | Digital India Programme," n.d., https://digitalindia.gov.in/content/programme-pillars.

iv Ministry of Electronics & Information Technology, "Approach and Methodology | Digital India Programme," n.d., https://digitalindia.gov.in/content/approach-and-methodology.

v "Full Text of PM Modi's Speech at UN," *NDTV.Com*, September 26, 2015, https://www.ndtv.com/india-news/full-text-of-pm-modis-speech-at-un-1223100.

vi United Nations, "Take Action for the Sustainable Development Goals," n.d., https://www.un.org/sustainabledevelopment/sustainable-development-goals/.

vii Unique Identification Authority of India, "About Your Aadhaar," 2019, https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html.

viii Government of India, "MyGov: An Overview," December 3, 2014, https://mygov.in/overview/.

ix Ministry of Electronics & Information Technology, "Welcome to CSC E-Governance Services India Limited," 2019, https://web.archive.org/web/20190909035106/https:/www.csc.gov.in/.

x NH Rao, "Digital Agriculture and Food Security: Framework for Integrating Agricultural Knowledge Services with Digital India" (National Academy of Agricultural Research Management, October 16, 2015), https://crispindia.org/wp-content/uploads/2015/10/Framework-for-Implementing-ICTs-in-Agricultural-Development-in-India-N-H-Rao.pdf.

xi "India Ranks 3rd among Nations Facing Most Cyber Threats: Symantec - ET CIO," *ETCIO.Com*, April 5, 2018, https://cio.economictimes.indiatimes.com/news/digital-security/india-ranks-3rd-among-nations-facing-most-cyber-threats-symantec/63621655.

xii "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar" (NSI, November 19, 2019), https://nsiteam.com/commodification-of-cyber-capabilities-a-grand-cyber-arms-bazaar/.

xiii "How India's Cyberthreats Are Evolving: Microsoft Security Team's Key Findings - India's Cyberspace at Risk," *The Economic Times*, July 31, 2020, https://economictimes.indiatimes.com/tech/internet/how-indias-cyberthreats-are-evolving-microsoft-security-teams-key-findings/drive-by-downloads/slideshow/77276142.cms.