IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Designing Security Policies to Reduce the Cyber Threats: A Case Study

Suraj Chandrakant Mohite
Student, Master of Computer Applications
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *The development of cyber security policies is an area of keen worldwide interest. Many countries are actively creating cyber security policies to manage their critical information infrastructures and their critical systems. Many developed countries have created comprehensive cyber security policies aimed at establishing effective national cyber security structures. Developing countries are also in the process of creating their own cyber security policies and frameworks, and these countries are in the position where they can harness the lessons learnt in developed regions. Most countries are grappling with how to handle cyber security issues, especially threats to critical infrastructure. In this special report we will design and discuss security policies in different countries to reduce the cyber threats.*

Keywords: Cyber Security, Cyber Crime, Threats; Cyber Lock, Loss After the Attack, Policies for the Countries, etc.

I. INTRODUCTION

The development of national cyber security policies and frameworks is on the agenda of many countries around the world. The development of such frameworks in countries which are growing rapidly, as these areas are experiencing growth in terms of the use of technology, the number of interconnected systems, and the number of users.

The development of cyber security policy documents and frameworks in developing countries should be aimed at producing holistic structures that can address both technological concerns. There are a number of cyber security policies that are being created in developing regions.

Traditional Critical Information Infrastructure Protection (CIIP) structures are largely driven from a governmental-level, however holistic structures (one that addresses all areas of society) are particularly attractive for use in developing regions due to the unique concerns exhibited in this deployment environment.

A primary component that is under investigation in this paper is to identify and protect the national security of the countries with the policies they have and what updates and new technologies they should adopt.

II. RANKING THE 10 MOST POWERFUL CYBER NATIONS IN THE WORLD

According to the team at the Belfer Center for Science and International Affairs at Harvard's Kennedy School, the most powerful cyber countries in the world are as follows:

1. United States.
2. China
3. United Kingdom
4. Russia
5. Netherlands
6. France
7. Germany
8. Canada
9. Japan
10. Australia

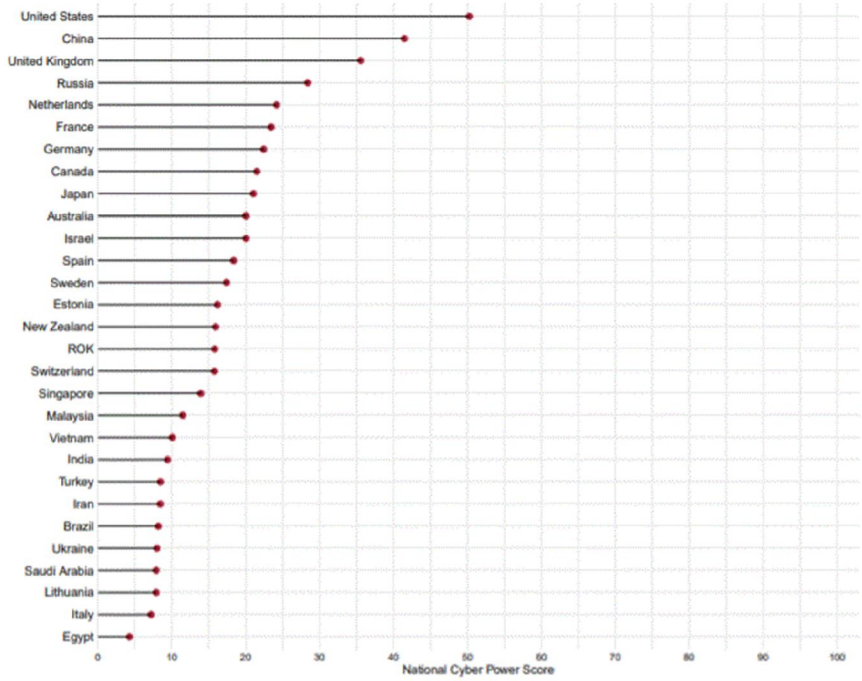
Surprised to see certain countries missing from the top 10 list?

Israel is listed as the eleventh most powerful nation in cyberspace, in a virtual dead heat with Australia. And Estonia is 14th. More on those two surprises later on.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Let's zoom out a bit and look at the top 30 global cyber power rankings:[1]

Graph 1: NCPI 2020: Most Comprehensive Cyber Powers



III. HOW WERE MOST POWERFUL CYBER COUNTRIES RANKED?

It is always fascinating to see "top ranking lists" like these, but how do we know what this really means, and what criteria did the Harvard researchers use?

Here's the short answer if you're a math geek:

$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{7}\sum_{x=1}^{7} Capability_x * Intent_x$$

And now, here is the explanation *the rest of us* can understand.

In determining the National Cyber Power Index (NCPI), the research team is taking what it calls an "all of country approach" to determining and ranking cyber power. The group identified seven national objectives that countries pursue using cyber means. [2]

The seven objectives are:[3]

1. Surveilling and Monitoring Domestic Groups;
2. Strengthening and Enhancing National Cyber Defenses;
3. Controlling and Manipulating the Information Environment;
4. Foreign Intelligence Collection for National Security;
5. Commercial Gain or Enhancing Domestic Industry Growth;
6. Destroying or Disabling an Adversary's Infrastructure and Capabilities; and,
7. Defining International Cyber Norms and Technical Standards.

IV. WHERE THE UNITED STATES LOSES TO CHINA AND RUSSIA IN CYBER POWER

Even though the United States is ranked number one overall, China continues to build on its cyber strengths. In several cyber power categories, it now leads the world. And in at least one instance, Russia also tops the United States.

- *Cyber surveillance power:* When it comes to cyber surveillance, China is the most powerful in cyber.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Researchers say Russia is second in the category and the United States is third.

- *Cyber power in commerce:* In this category, China is number one, the U.S. is second.

Researchers says China's intent here is clearly documented: "In-line with recent headlines in Western countries, China tops the Growing National Cyber and Technology Competence objective. Along with DPRK (North Korea) and Iran, China is one of only three countries assessed to be pursuing this objective through both legal and illegal means.
It has been both observed conducting industrial espionage and sought to incentivize and grow its domestic cyber expertise through research and development, and public-private partnerships."

- Cyber Defense Power: China is ranked number one in this category, followed by the Netherlands and France, then the United States and Canada.
- Additional Cyber Power Categories: Researchers concluded that the United States leads in cyber offense, influencing cyber norms, and cyber intelligence.

If this were a magic quadrant analysis, which is common in the cybersecurity industry, only five countries make it to that part of the plot, in the upper right here:

Graph 3: Plot of Cyber Power Rankings across Capability and Intent

V. THE REASON WHY US IS THE STRONGEST COUNTRY IN CYBER SECURITY

The United States of America is one of the nations that is encountering a huge number of cyber-attacks every year. That is the reason around 58% of the digital security organizations are situated there and endeavor to discover better approaches to battle with the most recent attacks. Among the methodologies that the nation has deployed is significantly encouraging policies and best practices. The government is constantly reassuring transparency, productivity and development with regards to data security. All the more along these lines, the government has been seen working with stakeholders in cultivating internet governance through the development of models and the dismissal of fake cyber security concerns.
The United States has attempted consolidated endeavors with accomplices in executing cyber security strategies, outlying cyber security principles, addressing cybercrime and protecting sensitive framework from cyber threats. It has been very much successful.[5]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

VI. CHINA IS MAKING SIGNIFICANT CYBER POWER GAINS

The Harvard researchers behind the National Cyber Power Index conclude that when it comes to cyber capabilities and the ability for a country to carry out national objectives through cyber, the United States remains the leader overall, but China is rapidly gaining:

"The US scores highest on five out of seven objectives... China is in the top 5 for every single objective. In recent years, China has invested heavily in research and development of technologies that allow the country to achieve multiple objectives in cyberspace. These results reflect China's increasingly dominant position in cyberspace but also highlight the significant gap in capability between China and the US in most areas."[6]

VII. THE REASON EGYPT IS WEAK COUNTRY IN CYBER SECURITY

In June 2020, at least 13 websites affiliated with the Ethiopian government were hacked and defaced. The targets were diverse, from seemingly innocuous sites such as Ethiopia's Educational Evolution Office, the Statistics Centre, and the National Lottery Administration, to more sensitive targets like the Police Commission and Ethiopia's Official Government Gazette. The "Cyber Horus Group," as the hackers called themselves, left nationalistic messages with pharaonic-themed inscriptions and music. The group wrote on the hacked pages: "If the river's level drop, let all the Pharaoh's soldiers hurry and return only after the liberation of the Nile." They warned, "engaging with Egypt in a war may cost you more than the lives of an Ethiopian people," and ended with the hashtags "#God_Bless_Egypt" and "#God_Bless_Egyptian_president."

The attack on these 13 Ethiopian government websites during a time of escalating tension between Ethiopia and Egypt demonstrates an emerging flirtation with offensive cyber tools as instruments of foreign policy—as well as Egypt's cyber limitations. As Egypt's crises with its immediate neighbors have mounted significantly in recent years, so too has the country's willingness to use subversive cyber elements for statecraft.

The defacements themselves were low-tech; the hacking and defacing of websites is a common and unsophisticated form of cyberattack. Government websites can be particularly vulnerable as they are oftentimes outdated and not well-maintained. However, despite the simplicity, low-tech operations can have serious consequences. In 2017, the relatively unsophisticated hack of state-owned TV station Qatar News Agency eventually contributed to a regional diplomatic rift. While many other developments established a strong prior willingness to excommunicate Qatar, the incident demonstrates the far-reaching repercussions of basic security vulnerabilities in the digital era.

Mounting evidence suggests that Egypt will put more cyber tools to use in the foreign policy arena.

Egypt's 2017–21 Cybersecurity Strategy also emphasizes the improvement of infrastructure to aid in the development of e-government services. While this is an important and necessary goal, increased digitization of government services simultaneously increases the government's vulnerability to attack. Moreover, it is unclear if adequate investments in basic cybersecurity and cyber defence have been made, as much of Egypt's basic national IT infrastructure is outdated. In comparison to cyber leaders in the region—such as Iran and Israel—Egypt lags woefully behind.

Given the clandestine nature of the field, it is impossible to determine the level of sophistication of the cyber weapons in Egypt's arsenal. However, the existence of sophisticated cyber weapons seems highly unlikely, as there is little evidence to suggest Egypt has the capacity or resources necessary to develop these capabilities in-house.

In the National Cyber Power Index (NCPI) that was released last summer by Harvard's Belfer Center, Egypt scored the lowest in comparison to the other 30 states surveyed. The NCPI, which scores both cyber intent and capability, found that Egypt has both a low capability and low intent to project cyber power. An important caveat, however, is that Egypt may simply not publish enough information about its cyber capabilities in order to be appropriately measured.

Egypt's cyber limitations could be due, in part, to a lack of human capital and necessary access to technical expertise and skilled employees. The institutional constraints of a rigid authoritarianism potentially hamper the necessary creativity and innovation zeal for progress in these domains. Additionally, unlike Iran, Egypt has enjoyed comfortable, long-term strategic alliances with global cyber powers like the United States that have helped to insulate the country and deter damaging state-backed cyber-attacks. Without a decade of relative diplomatic and multilateral isolation, Egypt did not experience similar existential and external incentives to develop its own domestic arsenal.

Most importantly, however, is that much of the country's cyber weapons and resources have been dedicated to repressing its own population. Egypt has been documented purchasing a range of sophisticated censorship and surveillance tools to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

control and suppress domestic political dissent, from deep-packet inspection censorship tech purchased from the Canadian-founded company Sandvine, notorious German-made FinSpy spyware produced by FinFisher, to the Italian manufactured Hacking Team surveillance tech—the most infamously disturbing technologies used for domestic repression have been procured by Egypt. When the state perceives its own population as a primary danger to national and digital security, few resources will be dedicated to combatting external threats. [7]

VIII. LITERATURE REVIEW

In recent decades, the number of scientific studies on cybersecurity problems has increased. Several can be identified, which focus on the formation of a security strategy at the country level. In determining the National Cyber Power Index (NCPI), the research team is taking what it calls an "all of country approach" to determining and ranking cyber power.Thus, Ghernouti-Hélie

(2010) explores some issues related to the deployment of a national cybersecurity strategy for the country in the context of its interaction with other countries. Galinec et al. (2017) on the example of the National Cyber Security Strategy of the Republic of Croatia and the Action Plan try to identify organizational problems in the process of their formation and provide recommendations for their solution. Teoh and Mahmood (2017) examine the relationship between national cybersecurity strategies and the digital economy and analyzes their impact on the success of the digital economy. Kshetri and Murugesan (2013) highlight key elements of national cyber security strategies and assess their impact locally, nationally and globally. Kostyuk (2014) explores the challenges facing countries in the context of the creation of an effective national cybersecurity system and emphasizes the need to develop a private-public partnership in this area.

This aspect is also considered by Štitilis et al. (2017), which analyzes national cybersecurity strategies for their compliance with cybersecurity policies and strategic areas of the EU and NATO. Jacobs et al. (2017) proposes as part of the country's cybersecurity strategy to create a cyber defense monitoring and incident response model based on integrating the country's military capabilities and cybersecurity operational models.

IX. CONCLUSION

The development of national cyber security policies and frameworks is high on the agenda of many countries, and developing countries are no exception. Once these policies are implemented it is likely that it could become a template for influencing similar policies in other countries in the same or different regions.

The US government is constantly reassuring transparency, productivity and development with regards to data security. That is the reason why US is number one strongest cyber secured country. Egypt government is lacking in human capital and necessary access to technical expertise and skilled employees. Egypt's basic national IT infrastructure is outdated. Mounting evidence suggests that Egypt will put more cyber tools to use in the foreign policy arena.

To this end, in this paper we outlined the cyber security policies of different countries to reduce the cyber threats and to developed a secured cybercrimes free country.

REFERENCES

[1] IEEE (ieee.org)
[2] SCI-HUB (https://sci-hub.hkvisa.net/)
[3] **INSPEC Accession Number:** 14528847, **DOI:** 10.1109/ISTAFRICA.2014.6880605
[4] **INSPEC Accession Number:** 13413108**, DOI:** 10.1109/MSP.2013.29
[5] www.secureworld.io/industry-news/top-10-most-powerful-countries-in-cyberspace
[6] https://www.analyticsinsight.net/top-6-countries-with-the-best-cyber-security-measures/
[7] https://timep.org/commentary/analysis/egypts-digital-foreign-policy/
[8] https://ieeexplore.ieee.org/Xplore/home.jsp
[9] **INSPEC Accession Number:** 19101116, **DOI:** 10.1109/CyberSecPODS.2019.8885271
[10] **INSPEC Accession Number:** 12172669.
[11] www.researchgate.net/publication/346482423_Strategy_for_Determining_Country_Ranking_by_Level_of_Cybersecurity
[12] https://seconcyber.com/cyber-security-developing-countries/