Can Fragile States Maintain Cybersecurity?

Donna M. Schaeffer
Marymount University

Rebecca Rohan
Marymount University

Patrick C. Olson
National University

Each year, Foreign Policy publishes the Fragile States Index, which ranks nation-states' sustainability in terms of political, economic, and social systems, as well as internal cohesion and the existence of external intervention. Sustainability and cybersecurity are topics of current interest, but they are rarely discussed together. It is pertinent to investigate whether fragile states can maintain cybersecurity during an era of disruptive technologies and as their economies experience digital transformation. In our global society, cybersecurity is an increasing concern. Our study compares the countries on the 2021 Fragile States Index with rankings on the National Cyber Power Index published by the Belfer Center for Science and International Affairs at Harvard University. The most fragile states are not well prepared in the realm of cybersecurity. We identify how various indicators on the Fragile States relate to cybersecurity capacity building. This introductory paper is the first in a series.

Keywords: cybersecurity, sustainability

INTRODUCTION

A nation's political, economic, and social systems' sustainability is critical to maintaining its status as an independent entity in the world order. Key definitions are provided. We then introduce the concept of cybersecurity and the important role it plays in a nation's sustainability. The methodology section explains where and how the data is gathered. The results section describes the findings.

Definitions

Albertson and Andrews (2017) describe a fragile state as one that has lost control of its territory or one that cannot provide basic services to its citizens. Typically, fragile states do not have governments with legitimate authority or practice collective decision-making. For a variety of reasons, fragile states may not be able to interact with other states in the global community. A fragile state may experience corruption and criminal behavior in its ruling body and inequality amongst demographic groups.

The Fund for Peace has identified five groups of key factors that can provide insight into a state's fragility or sustainability. The groups are Cohesion, Economic, Political, Social, and Cross-cutting indicators. As an example, Table 1 shows the connections between Cohesion indicators and cybersecurity.

TABLE 1
COHESION INDICATORS AND CYBERSECURITY

Indicator	Connection to Cybersecurity
Security apparatus	1. Cyberwarfare 2. Cyberterrorism 3. Cybercrime 4. Cyber espionage against citizens
Factionalized elites	1. Disinformation and Misinformation 2. Cyberbullying against minorities, e.g., religious or ethnic groups
Group Grievance	1. Propaganda

The second key factor in measuring fragility is a state's economy. Table 2 shows the cybersecurity issues that are related to economic indicators. These indicators are related to the cybersecurity readiness and capacity of a state.

TABLE 2
ECONOMIC INDICATORS AND CYBERSECURITY

Indicator	Connection to Cybersecurity
Economic Decline and Poverty	1. Cybercrime 2. Decline of Cybersecurity Startups 3. Closure of Cybersecurity Businesses 4. Enrollment Decline in Cybersecurity Programs at Undergraduate and Graduate Levels
Uneven Development	1. Lack of Diversity in Cybersecurity Programs at Undergraduate and Graduate Levels 2. Lack of Diversity in the Cybersecurity Workforce

Indicator	Connection to Cybersecurity
Human Flight and Brain Drain	1. Skilled Cybersecurity Workforce Leaving the Country 2. Students Attending Undergraduate and Graduate Programs in Other Countries

The political environment of a state plays a key role in determining its fragility, and also its cybersecurity posture. Table 3 identifies some connections between political indicators and cybersecurity. Issues such as election security, which is a current topic, impact the fragility of a state

TABLE 3
POLITICAL INDICATORS AND CYBERSECURITY

Indicator	Connection to Cybersecurity
State Legitimacy	1. Cyber Tampering in Elections 2. Social Media Attacks Against the Government
Public Services	1. Equal Access to the Internet 2. Cybersecurity Programs Accessible to All Interested Students
Human Rights and the Rule of Law	1. Cyber Bullying 2. Freedom of Speech and Freedom of Religion not Censored on Social Media or the Internet 3. Media Free from Government Influence 4. Equal Access to the Internet and Information

The fragility of a state can be assessed via several social indicators. Table 4 connects two social indicators with cybersecurity issues.

TABLE 4
SOCIAL INDICATORS AND CYBERSECURITY

Indicator	Connection to Cybersecurity
Demographic Pressures	1. Internet Sustainability—support growth in terms of people accessing the infrastructure
Refugees and Internally Displaced Persons (IDPs)	2. Internet Access 3. Cyber Bullying 4. Disinformation and Misinformation

Finally, the cross-cutting indicator of external interventions is related to cybersecurity in terms of cyberwarfare, as indicated in Table 5.

TABLE 5
CROSS-CUTTING INDICATORS AND CYBERSECURITY

Indicator	Connection to Cybersecurity
External Intervention	1. Cyber Warfare 2. Cyber Espionage 3. Disinformation and Misinformation 4. Propaganda

METHODOLOGY

As this is an introductory exploratory study, we obtained the Fragile States Index and the National Cyber Power Index. We connected the indicators on the Fragile States Index to cybersecurity issues based on our expertise in the cybersecurity profession and current topics that are receiving media attention, e.g., election security and human rights. Then we investigated the relationship between a nation's ranking on the National Cyber Power Index and the Fragile States Index. We next plan to review the literature on each indicator and cybersecurity issue. The analysis phase will attempt to define a relationship between a nation's ranking on the Fragile States Index and the National Cyber Power Index.

Results

The National Cyber Power Index published by the Belfer Center for Science and International Affairs at Harvard University ranks cyber-powerful counties based on a multitude of indicators, including several that are considered in the Fragile States Index. These include a state's capacity to: surveil and monitor domestic groups, control and manipulate the information environment, and collect foreign intelligence for its national security. Being a player in establishing technical standards gives countries power to develop a

thriving and robust . . . cybersecurity industry. Cyber power is viewed from both defensive and offensive postures.

Table 6 lists the ten most cyber-powerful countries and their ranking on the Fragile States Index. It is interesting to note that the top countries in cyber power rank fairly low on the Fragile States Index.

TABLE 6
COMPARISON OF RANKINGS

Ranking per National Cyber Power Index	Ranking per Fragile States Index
1) United States	143rd
2) China	95th
3) UK	150th
4) Russia	74th
5) Netherlands	168th
6) France	159th
7) Germany	167th
8) Canada	171st
9) Japan	161st
10) Australia	170th

DISCUSSION AND FUTURE RESEARCH

The 2021 Fragile States Index ranks Yemen as the most fragile state among the 179 countries it measures (Fund for Peace, 2021). The civil war has created humanitarian and infrastructure problems. Lingaas (2018) reported that cyber warfare is an important component of combat there. When the opposition gained physical control of Sanaa, Yemen's capital of Sanaa, they took kinetic control of the country's internet backbone turning it into YemenNet. Experts say vulnerabilities exist because the hardware and firmware are manufactured in China. The existing government countered by establishing

AdenNet, its Internet Service Provider (ISP). Researchers at Recorded Future and VirusTotal have found increases in viruses and malware on this network (Lingaas, 2018).

The Fragile Stats Index also highlights countries with the largest changes in their fragility in both positive and negative directions. For example, in 2021, the United States saw the largest year-to-year worsening in its fragility. Analysts speculate police violence, election insecurity, and the impacts of the Covid-19 pandemic were major contributors to the decrease. We acknowledge cyber threats against United States systems are increasing in number and severity, and discuss the role important cybersecurity topics, such as disinformation and misinformation, have on the nation's rankings.

Future research is needed to validate the assumptions we have made regarding the cybersecurity implications of the indicators. Additionally, we plan to identify correlations among a nation's rankings on both Indice. We believe that nations with high ranks on the Cyber Power Index will be ranked low on the Fragile States Index, and vice versa.

REFERENCES

Albertson, A., & Moran, A. (2017). *Untangling the Complexity of Fragile States.* Truman Center. Retrieved from https://www.strausscenter.org/wp-content/uploads/Untangling-the-Complexity-of-Fragile-States-2017.pdf

Caramancion, K.M., Li, Y., Dubois, E., & Jung, E.S. (2022). The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats. *Data*, *7*(4), 49.

Dawson, M., Tabona, O., & Maupong, T. (Eds.). (2022). *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security*. IGI Global.

Fund for Peace. (2021). Fragile States Index. Retrieved from https://fragilestatesindex.org/global-data/

Lingaas, S. (2018, 28 November). How Cyberwarfare is Playing Into Yemen's Civil War. *Cyberscoop.* Retrieved from https://www.cyberscoop.com/yemen-civil-war-cyberwarfare-recorded-future-cyberwarcon/

Messner, J.J. (2020). *Fragile States Index Annual Report 2020*.

Shackelford, S., Raymond, A., McCrory, M.A., & Bonime-Blanc, A. (2022). Cyber Silent Spring: Leveraging ESG+ T Frameworks and Trustmarks to Better Inform Investors and Consumers about the Sustainability, Cybersecurity, and Privacy of Internet-Connected Device. *Cybersecurity, and Privacy of Internet-Connected Devices*.

Tijerina, W. (2022). Industrial policy and governments' cybersecurity capacity: A tale of two developments? *Journal of Cyber Policy*, pp. 1–19.

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., & Schwarzenbach, A. (2020). *National Cyber Power Index 2020*. Belfer Center for Science and International Affairs, Harvard Kennedy School.