Building a Cyber-Secure Culture: How Enculturated Behaviors Affect Cyber-Security Concerning Nation-States and Businesses

Jali Purcell

Drury University, Springfield, MO
Fuse 201: Introduction to Intercultural Communications
December 16, 2022

Abstract

The research and development completed on how cultural behaviors affect cyber-security fulfill the final project in Fuse 201: Introduction to Intercultural Communication. Through participation in this class, background knowledge about how cultures differ from each other on an international, national, and sub-national was obtained preceding the research. Two semesters' worth of cyber-security credits gave the background knowledge about the importance of information security in businesses.

The main research questions I focused on were how countries establish international laws of cyber-security, as well as which nations are leading by example for other nation-states to follow. To complete this, I made an interactive map that could serve as a prototype for a website that displays information about how a country's state of cyber-security.

To better apply to the average user, I read reports about at how businesses should incorporate cyber-secure practices in the workplace. The key research questions were about how cyber-security programming should be adapted to complement the businesses' cultural composition. Suggestions are made for how to adapt programming for the behavior that is most infringing on cyber-secure behavior.

The research on these topics can help citizens be aware of how cultural differences affect cyber-security. Business owners may be especially interested in the research done about cyber-secure awareness programs in the office.

1 Introduction

According to Mattias C. Kettemann in his article "Ensuring Cybersecurity Through International Law", "Cybersecurity is defined very broadly by some states, and covers risks and threats such as cyberwarfare, cyberterrorism, cybercrime and cyberespionage" [1]. The report continues to explain how cybersecurity must be incorporated into a nation's defense policy, despite their definition of cyber-security. Attacks are

not the only thing that threatens a country's cybersecurity. It is dangerous as well to have weakness in areas "such as developing crisis intervention centers and teams, as well as transnational crisis communication structures for cyber incidents" [1]. In other words, it is a country's responsibility to invest in cyber-threat defense, crisis response teams, and education of its citizens in regard to cyber-attacks.

How do nation-states promote cyber-secure behaviors? Which nation-states are good examples for others to learn from? By comparing statistics given by Comparitech, this question can be explored [2]. While there are other ranking institutions, some of which place the top spot for a different candidate, this ranking was the most updated and thorough with their explanations, as well as providing a link to where they got their data.

The average user may not be able to apply some of the more advanced techniques for cyber-security that nation-states must. It's more likely they'll encounter the choice to be cyber-secure in their free time browsing the internet, or at their job. Companies that do not prioritize cyber-security are bound to run into some problems, not just from attacks, but from the threat of insecure employees. Even if they do bring awareness to cyber-attack strategies such as phishing, or social engineering, good programs must be tailored to the workplace's culture in order for employees to care enough to learn about the material.

Which behaviors should business owners be aware of when making their cybersecurity awareness programs? Are there any cultural behaviors that could make a positive or negative impact on the willingness to adopt cyber-secure behavior?

2 Nation-State Involvement in Cyber-Security

The most critical cyberterrorist attacks are brought on by individual countries and are known as nation-state attacks. "Historically, nation-state actors directly targeted infrastructure, think tanks, and governments of other countries" [3]. In this scenario, a nation-state actor means they are the one with the intent to damage another organization with cyber-crime. There have been a few attacks in the past that demonstrates how necessary it is to have an international set of standards. When the Ashley Madison website, a website containing clients in marital relationships to form extramarital connections, was hacked, the information contained from their clients was used as blackmail for members of the U.S. military [4].

Information for blackmail is not the extent that hackers can reach. They can also attack critical infrastructure. For example, in 2010, a computer worm first named "Stuxnet" was sent to attack the Iranian nuclear facilities. It was able to be injected via a USB and then could verify if the computer was a target or not. This caused the centrifuges controlling the materials for their nuclear system to spin out of control and explode [4]. The damage they committed sent their progress back by a few years. An attack this advanced had to have cooperation from a nation-state. Many suspect the United States and Israel, but neither nation has taken responsibility for it.

A conflict between nation-states in cyber-space must be met with some way to establish international guidelines. Although the definitions of what constitutes as an attack may differ between countries, nation-states must be "responsible to the international community with regard to cybersecurity according to their judicial authority over critical infrastructures pertinent to it" [1]. Kettemann suggests the best way to set precedent against attacks such as these is to create an international set of guidelines. Having existing laws to turn to is the best way to reduce risk and establish security goals.

2.1.1 Construction of Cyber-Security Norms.

The *UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International* Security calls for the construction of globally accepted norms for cybersecurity [1,4]. While the content of such norms may be debated, having these norms received and implemented correctly by nation-states' different cultures is a challenge in itself. "Fortunately, the social science literature has already explored a diverse array of norm-construction processes. That literature offers useful lessons missed if one examines cybernorms only as products" [4]. Just as social norms such as table manners are enculturated into a group, so should these norms for cybersecurity be structurally enculturated into society.

Each norm has four parts for application: identity, behavior, propriety, and collective expectations. Identity refers to who it applies to, whether it be the whole country or banks in general. "Norms may even arise for bilateral pairings of states, as witnessed by China's recent agreement on a norm against cyberespionage for commercial purposes with the United States" [4]. In this example, the identity of the norm applies to the joint agreement between the United States and China. More specifically, the institutions in place that handle their commercial sectors.

Behavior refers to the actions that encompass the norm. What is prohibited or allowed with this particular norm? For example, "The U.S. Federal Trade Commission, for example, recently adopted a standard-based approach in directing companies holding third-party data to have "reasonable" cybersecurity" [4]. Given the background of the identity, certain behaviors may already be in place that can be evolved for the context of the cyber-security realm.

Propriety determines when norms can label behavior as appropriate or not. The clearest propriety is within a law. "One goal of those who make law (or conclude treaties) is to establish norms" [4]. A law may be the best avenue to definitively set norms to expectations. Just as nations have their own laws, cyberspace will have its own set of norms, codified somewhere universally such as with the UN.

Collective expectations refer to the social characteristic of norms. When laws are established, they create a collective expectation. To truly take effect, norms need to be understood by who it applies. "Norms are what social scientists call social constructions. They exist only because we all believe they exist" [4]. The power we give to money, which is essentially a piece of paper, is a social construct. Just as different cultures have enculturated certain behaviors into their groups, norms will need to be enculturated into different societies to truly take international effect. Commitment to the norm needs to be sincere, which may prove to be a tough task to complete.

2.2 Research and Development in Nation-State Comparison.

When nations impose these norms, either at an international or national level, their cyber-security score will reflect how well they are at getting their culture to adopt cybersecurity norms. Which states provide a good example to others who are struggling to get their culture to adapt? A possible solution to this would be an in-depth website, showcasing where each nation stands, what strides they have made, as well as what norms they have adopted into their laws. It could also be used to let others be aware of the risks they have when entering the cyberspace, or physical space, of some of the less secure countries.

In creating such a website, a lot of input from other countries would be necessary. Given the time allotted for this research project, I was only able to come up with a single map. Given statistics based on Comparitech's rankings, each of the countries they rank is

attached to a label with their score, as well as their highest level percentage of insecurity. “Each year, our study looks at over 60 countries to find out where in the world you’re most ‘cyber safe’ [2]. The categories in which Comparitech ranked the now 75 countries include categories such as “% of mobiles infected with malware”, “% of users attacked by ransomware trojans”, “% of attacks by cryptominers”, and “the best-prepared countries for cyberattacks” [2]. For each country, I wanted to display a portion of their data.

In creating such a website, a lot of input from other countries would be necessary. Given the time allotted for this research project, I came up with a very early version of the website. Based on Comparitech’s data, each of the countries are attached to a label with their score, as well as their highest level percentage of insecurity. A more in-depth website would provide more information.

To compare this to a cultural aspect, I have included a column for the type of government from the World Population Review [5]. While this data does not always guarantee that a country is either authority-ranking or egalitarian, it can at least provide a way to compare the data based on a national influence on culture.

The prototype of the website was coded using R. R is a programming language focused on data analytics and statistical analysis. There are built-in packages that can produce high-quality, visual representations of data. Excel was used to organize the countries from best to worst scoring, then added an extra variable for the rank. The CSV output was used as input for the R program. To give context to the viewer, the worst category from each country was found by seeing which percentage was the highest of the categories that Comparitech scored on. Here is a screenshot from the published result.

FIGURE 1: Map created by the R Programming Language that gives a prototype for a website detailing the level of cyber-security and government type for the nations ranked by Comparitech. Link to Website

2.2.1 Results Analysis

In the textbook, *Understanding Global Cultures: Metaphorical Journeys through 34 Nations, Clusters of Nations, Contents, & Diversity*, the differences between egalitarian societies vs. authority-ranking societies are documented. In a paternalistic authority-ranking society, there is a chain of responsibilities. Those lower in a hierarchy respect those above them, and in turn, those who are at the top provide for those below them. In an egalitarian style of society, this hierarchy is not as influential. Strict structures of formalities that exist in an authority-ranking culture are not always followed in an egalitarian culture [6].

If someone wanted to quantify how this cultural difference affects the score received by Comparitech, they could take the average score received by each structure of government represented, and compare them. For example, using the data from the website, this bar graph shows the comparison between countries listed as monarchies, relating to authority-ranking societies, and republics, relating to egalitarian societies. One-party states and absolute monarchies may represent a more authoritarian culture.

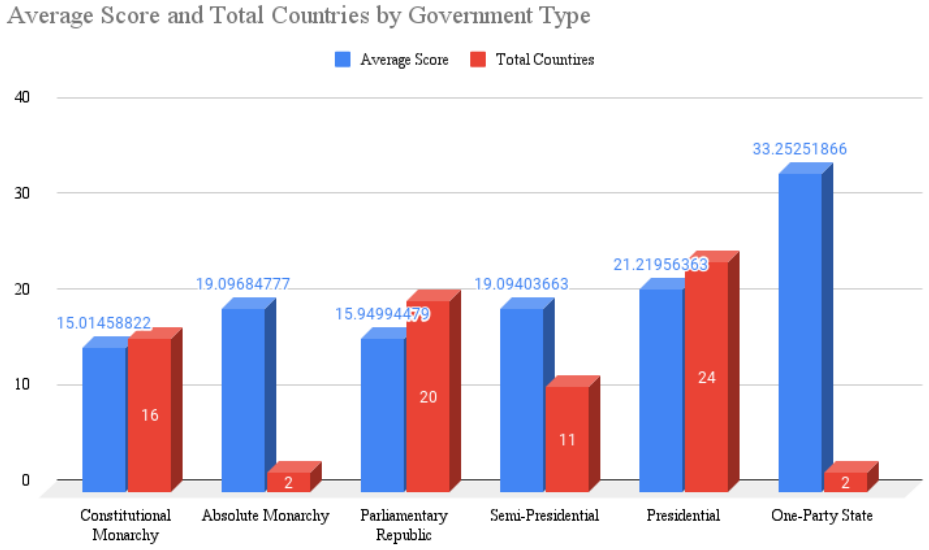

FIGURE 2: Average score and total countries comparison by government type.

These numbers were calculated by taking the total of the average score column for each government type, then dividing it by the total number of countries for each government type. These results show that on average, constitutional monarchies had the best rankings since a lower number indicates a better score. The lowest-ranking government type was one-party states, followed by presidential republics. The specific column calculations are shown below. The functions were completed in Excel, but a shareable link to the Google Sheet used to create the bar graph is included below.

Country	Government Type (wikipedia)	Government Type (world population review)	Average Overall Score	Total World Pop.	Average Score	Total Countires	Government Type
Denmark	Constitutional monarchy	Constitutional monarchy	3.557042198	240.2334116	15.01458822	16	Constitutional Monarchy
Sweden	Constitutional monarchy	Constitutional monarchy	4.904438693	38.19369553	19.09684777	2	Absolute Monarchy
Ireland	Republic	Parliamentary Republic	5.052696571	318.9988958	15.94994479	20	Parliamentary Republic
Norway	Constitutional monarchy	Constitutional monarchy	5.614011945	210.0344029	19.09403663	11	Semi-Presidential
Finland	Republic	Parliamentary Republic	6.357600922	509.2695272	21.21956363	24	Presidential
Netherlands	Constitutional monarchy	Constitutional monarchy	6.547595788	66.50503731	33.25251866	2	One-Party State
Austria	Republic	Parliamentary Republic	9.051290957				
United Kingdom	Constitutional monarchy	Constitutional monarchy	9.604753708				
Switzerland	Republic	Parliamentary Republic	9.918066566				
Croatia	Republic	Parliamentary Republic	10.18288035				
Haiti	Republic	Semi-Presidential	11.22753048				

FIGURE 3: Calculations done in Excel to find the government type with the best average score. Link to Google Sheet

The top two countries are listed as constitutional monarchies, with the top spot given to Denmark. Denmark's cyber-security has improved immensely since the 2016 attack on the US Democratic Party revealed sensitive information on members of the Danish Defense, according to an article published in the International Journal of Politics, Culture, and Society. According to the article, the Danes are particularly good at "individual user hygiene and financial services security" [7]. The success was drawn own by nationwide two-factor authentication. This refers to the secure practice of requiring an additional authentication method. If a hacker were to obtain a password to a website, if the victim used two-factor authentication, the hacker would be stopped from getting into the account if they did not have access to their other identity token, often generated via email.

In contrast to very individualist, egalitarian societies such as the United States, the widespread adoption of two-factor authentication seems like an impossible feat. According to a survey done by SecureAuth, a leading company in the realm of user authentication out of California:

> When considering the impact on end users, 74 percent of respondents who use 2FA admit that they receive complaints about 2FA from their users – and nearly 10 percent of them just "hate it." This is a noticeable turnaround from a 2016 SecureAuth survey, which revealed 99 percent of IT departments believed two-factor authentication was the best way to protect an identity and its access [8].

While IT departments are aware that the most secure practice is to adopt two-factor authentication, it has been a challenge to get users to accept the change.

In the case of Denmark, they could have used their cultural behaviors to their advantage. While they are an individualist society, their individualism is unique in that they have a high level of "societal institutional collectivism practices" [6]. This could be the key to how Denmark was able to get two-factor authentication accepted into their society: if everyone collectively agrees on an institutional change for the benefit of the community, they will adopt the behavior. The burden of the extra steps it takes to log in is not outweighed by their ambition to be more secure as a whole. By educating citizen knowledge and improving cooperation between groups of actors, the Danish government succeeded in placing itself as a top-ranking nation in the realm of cybersecurity.

How does a true, collective, and authority-ranking country handle cyber-security? Take Thailand for example. They are ranked 34, 11 places above the United States in the Comparitech ranking [2]. According to a presentation done by the Electronic Transactions Development Agency, Thailand's agency to regulate e-transactions, improve laws, and encourage citizens to learn more, there are a few ways that they handle cyber-security [9].

One example is ThaiCERT, a response team under the direction of ETDA that handles incident response for cyber-crime. This group offers its services to the public and private sectors [9]. Given their authority, everyone is expected to follow the laws that they have helped to implement.

An example of these laws is the Computer-Related Crime Act B.E. 2550 [9,10]. This law is especially unique. It is a law containing rules about what constitutes as an illegal practice on computers, such as access to a computer by an unauthorized user. Looking into the specific sections of the law, readers can see the level of authority Thailand is imposing on the country. For example, in Section 16:

> Whoever enters a picture of another person into computer system where such picture was created, edited, added or amended electronically or by any other means in a manner which is likely to cause such other person to be defamed, denounced, detested or humiliated, shall be liable to an imprisonment for a term not exceeding three years and a fine not exceeding Two Hundred Thousand Baht [10].

For context, this fine is equal to 5,748.78 USD. So, if anyone were to photoshop a picture of someone that could cause humiliation, they go to jail and get a fine. In the United States, retouched images could be protected by the first amendment to free speech, if they are not classified as defamatory. However, in cases of only humiliation, no such fine applies to citizens living in the egalitarian society of the US. It is likely that retouched images would be handled on a case-by-case basis instead of a single law dictating any and all like this Thai example.

But this law, as well as the debate around whether each of these sections is too restrictive on the country, shows an example authority-ranking style of government regulating cyber-security laws. Since this act was produced by King Bhumibol himself, those respecting his authority would follow this law. While an individual's freedom to produce falsified content is taken away, the cyber-security for the nation improves.

3 Culture's Effect on Cyber-Security in the Business Sector

When looking at this data, one may feel like the role they have in being cyber-secure may not have a big impact. However, this is not the case. Adopting cyber-secure behaviors is important for everyone accessing the internet. While much of the Comparitech ranking focused on how well different nations prevent these attacks, another factor is how vulnerable or unaware individuals are when receiving an attack [2]. For example, some attacks are simulated by sending a malicious link containing code that attacks the user. A user must be aware of what these cases look like in order to prevent potential damage.

Cyber-security is especially important for companies. Companies that have customers often store a lot of customer data. This could contain sensitive information such as credit card numbers. Attacks on these companies can result in a data leak, putting a lot of others' assets at risk. Just as nation-states have to enculturate norms into their national culture, companies are responsible for providing their company with programming to teach them how to avoid, or be aware of attacks. That starts by educating employees in a way that they will intentionally make a change to their behavior.

3.2 Adapting Cyber-Security Programming

As companies exist around the world, each program must be adapted for their culture, including their enculturated behaviors. The specific behaviors that company owners should be aware of have been studied, especially in an article by representatives from the Cyber Security department at Oxford titled "Cyber Security Awareness Campaigns: Why do they fail to change behavior?" In the abstract, they describe that the goal of their project was to identify why cybersecurity programming fails to change behavior. Just because someone is aware of the risk, does not automatically mean they will make the changes to their habits [11]. So what will convince them? How should cybersecurity programming be tailored to fit the culture existing within a company?

This study picked out a few ways to distinguish cultures from each other including individualism vs. collectivism, masculinity vs. femininity, and uncertainty

avoidance. A company will need to reflect on which of these best describes their company in order to make their programming more accessible to them. “For example, in cyber security, a message used in a Western country would tend to avoid presenting the general risks of not being secure online and rather focus on the benefits of being secure” [11]. However, when presenting cyber-security programming to a more collectivist culture, it’s best to focus on what negative outcomes could arise for the group if an individual does not comply with the behavior.

The case study they looked at was the specific language used in cyber-security programming in the United Kingdom and Africa. In the United Kingdom, their core messages included telling individuals how to protect themselves and placing the responsibility for their online behavior solely on how they act online. In the contrasting African collectivist communities, cyber-security campaigns focused on how being cyber-secure can benefit everyone, as well as reminding people that not everyone is who they say they are online [11]. Each of these campaigns promotes a similar interest, but specifics about the goal of being safe online are different, as well as the way in which these messages are said to convince their respective cultures.

In a business context, if a program does not reflect what the culture of the company values, the genuine interest to comply with the standards set by a company significantly decreases. Another attribute that can contribute to the intention to comply with cyber security standards is their perceived control or the level at which the subject feels that they can control their own safety. “We suggest that a campaign should use simple consistent rules of behavior that people can follow. This way, their perception of control will lead to better acceptance of the suggested behavior” [11]. What these behaviors are is up to the company’s owner or their cyber-security leader, but analysis will be needed in order to accurately attune their education to their culture.

3.2.1 Perceived Control’s Effect on Cyber-Secure Behaviors

One study titled “Exploring the effect of uncertainty avoidance on taking voluntary protective security actions” found that the most impactful cultural behavior was uncertainty avoidance. They acknowledged other factors, even explaining how these factors can influence willingness to comply, such as masculinity-femininity referring to competitiveness vs. compassion. However, their study took a more direct approach in looking into uncertainty avoidance, because “Interestingly, information systems researchers (more broadly than just security researchers) have consistently reported that the uncertainty avoidance cultural dimension is the most influential cultural dimension in explaining the variance in a variety of technology related phenomena” [12].

In order to study the difference, they looked at the voluntary willingness to use a password manager to store longer, safer passwords. “The core idea behind this cultural dimension is that groups of people are socialized to have different levels of comfort with ambiguity and uncertainty” [12]. Depending on how people were enculturated to either manage or avoid uncertainty will affect if they voluntarily use a password manager or not.

The first thing they noted was that high uncertainty avoidance cultures accept new technology slower, waiting for others to adopt it first. Low uncertainty avoidance cultures are more comfortable with taking a risk to try new technologies. For high uncertainty avoidance participants, it would work better to focus on the level of threat that not having a password manager creates, instead of the newness of the technology. For this reason, their hypothesis was that individuals with higher discomfort with uncertainty would be more willing to adopt a password manager. The study surveyed 227 undergraduate business students from private US universities. There was a variety of cultures represented, including Asian, European, Middle Eastern, and North American participants.

However, the results ended up being negative instead of positive. They theorized

that this was because of the newness of the password managing technology, as well as the uncertainty related to the threat of a compromised password. So, the high uncertainty avoidance participants perceived that the more uncertain avenue was to use a password manager, where all passwords are stored in one place [12].

Putting this in the business context, if a manager felt more comfortable with having their employees store all their passwords in one safe location, they would need to first address how their company reacts to uncertainty. If they have a low tolerance for the unknown, the manager would need to create cyber-security programming showing how approachable and secure using a password manager can be. They would also benefit from highlighting how the other option of not using a password manager is riskier, since it puts all of the responsibility on the user to remember their passwords and store them safely, which could result in weaker passwords used for convenience's sake.

If their company has a high tolerance for uncertainties, they may have better luck at adopting the technology itself. They may have less luck at getting people to realize the level of vulnerability not having one creates, so it may be better to take the route of explaining the benefits of using a password manager, such as not having to remember several different passwords.

This cultural behavior is just one of many that a company will need to be aware of in order to make effective cyber-security programming. As Aurigemma and Mattson write:

> As with most other cross-cultural research, the main practical contribution of our study is that it is important for information security managers to know the composition and behavioral orientations of the people receiving security-related training in order to maximize their effectiveness… Particularly in culturally diverse organizations, ignoring the effect of cultural dimensions such as uncertainty avoidance, and possibly other cultural characteristics, can have a deleterious impact on the overall organizational information security posture [12].

Just as national cyber-security agencies have the responsibility to create relevant laws to protect their citizens from cyber-attacks, companies have the responsibility to review their own company's cultural composition and tailor their cyber-security programming to the existing behaviors of their employees.

4 Conclusions

When it comes to cyber-security, everyone has an impact on the level of security produced by a country. The most critical attacks are those supported by nation-state actors. In order to decipher what is considered legal or illegal cyber-attacks on an international scale, nation-states need to adopt an international list of norms. The way that these are engrained into the applicable identities is similar to any norm enculturated in a society.

How well countries are at adapting their country to these cyber-security norms can be studied by ranking institutions such as Comparitech. The prototype of the website I created can serve as a blueprint for making a more inclusive, accurate representation of the state of cyber-security on a global scale.

Just because nation-states are the ones creating these norms does not mean that individual citizens do not make an impact on cyber-security. Norms must exist in workplaces too. In order for managers to successfully enculturate cyber-secure behavior in their company, they need to make programming that is reflective of their company's culture. When nation-states and businesses are more aware of their culture, they can better adapt the way that they spread messages promoting cyber-security, and set up a more cyber-secure environment for everyone.

References

[1] Kettemann M. Ensuring cybersecurity through international law. *JStor* 2017.

[2] Bischoff P. Which countries have the worst (and best) cybersecurity? *Comparitech* 2022.

[3] Jones E. How nation-state attackers like nobelium are changing cybersecurity. *Microsoft Security Blog* 2021.

[4] Finnemore M, Hollis D. B. Constructing norms for Global Cybersecurity. *JStor* 2016.

[5] Republic Countries 2022. World Population Review.

[6] Gannon M. J., Pillai R. *Understanding Global Cultures: Metaphorical Journeys through 34 Nations, Clusters of Nations, Continents, & Diversity*. Sage, 2016.

[7] It decision makers reveal Two-factor authentication dislike and rise in adaptive authentication adoption. *SecureAuth* 2022.

[8] Venkina E. How Denmark became the most cyber-secure country. *How Denmark became the most cyber-secure country – Work and digitalisation | IPS Journal* 2021.

[9] Chaichana M. Thailand Cybersecurity Challenges and Risk Aspects. *หน้าแรก - สพธอ* 2022.

[10] Bhumibol A. Summary laws and rules. *Thailand National Trade Repository* 2017.

[11] Bada M, Sasse AM, Nurse J. R. C. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *arXivorg* 2019.

[12] Aurigemma S, Mattson T. Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. Elsevier 2017.