2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Internet as a CII - A Framework to Measure Awareness in the Cyber Sphere

Assaf Y. Keren
Communication and Cyber
Intelligence Solutions
Verint Systems
Herzliya, Israel
Assaf.Keren@verint.com

Keren Elazari
Communication and Cyber
Intelligence Solutions
Verint Systems
Herzliya, Israel
Keren.Elazari@verint.com

Abstract: With the increasingly vital role that the Internet plays in the personal lives of people across the world, Internet services have proliferated to such a degree that the Internet now equals countries' critical infrastructures in importance. In fact, some countries include Internet services in their legal framework for critical-infrastructure protection (CIP). In this paper, we take the view that the level of awareness and susceptibility to cyber attack can be measured by the level of maturity and development of the internet infrastructure of a country.
Using publicly available metrics, this study quantifies critical levels of Internet infrastructure across countries and proposes the cyber-attack susceptibility (CAS) index based on Internet usage, online services rendered, telecommunication infrastructure, and the human information-technology capital of each measured country. The information is used to further examine potential correlations between a country's critical Internet-infrastructure level and the country's ability to deal with cyber threats and the steps already taken by several high scoring countries in order to defend against attacks on Critical Infrastructure.

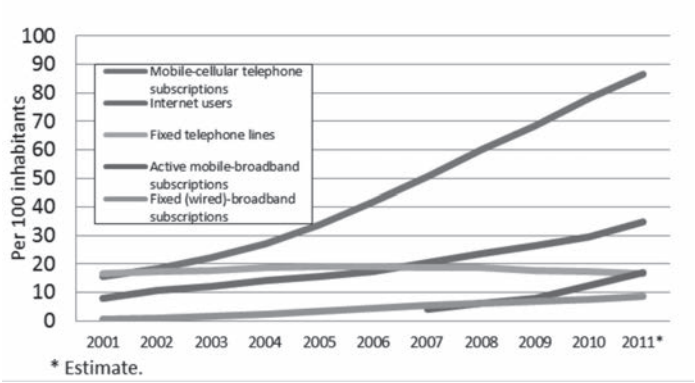
Keywords: *Internet; critical infrastructure; e-government*

1. INTRODUCTION

Over the last decade, the logarithmic scale of technology change has brought us into the information age in full force. One of the phenomena that this age has ushered in is the constant threat of cyber attacks - malicious attacks against computers and computer users. We are also witness to organized efforts by countries to develop the capability to attack other countries in the cyber sphere for the purpose of information gain or sabotage. This environment has led to the coining of the term *critical-information infrastructure*, an infrastructure that sustains life and must be defended against cyber attacks.

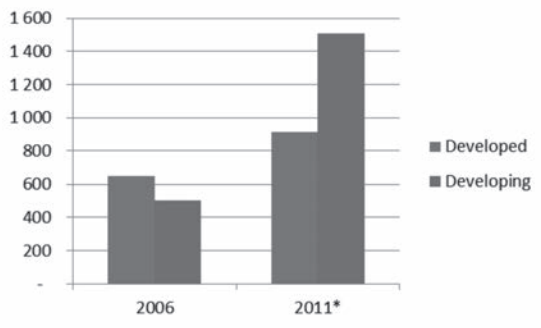
One of the biggest drivers of this was the creation and widespread proliferation of the Internet. Looking at data on global information and technology (ICT) developments [1], we can see constant growth in Internet and mobile-cellular telephone subscriptions over the 10-year period ending in 2011 (Figure 1).

FIGURE 1. GLOBAL ICT DEVELOPMENTS, 2001-2011.



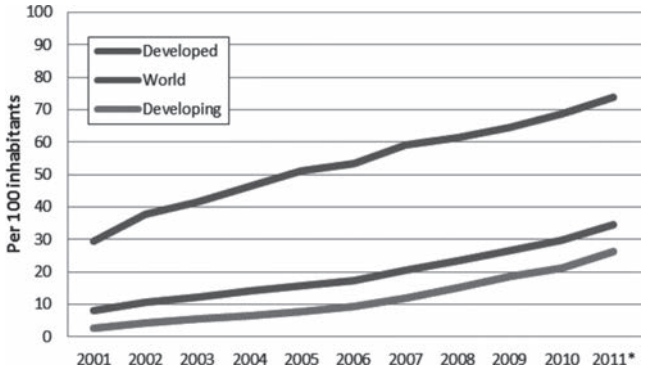
Moreover, the increase in Internet access is occurring not only in developed countries but also in developing countries [2] (Figure 2). As the latter race ahead with an ever greater number of Internet connections while disregarding issues such as proper infrastructure development and security, these countries' ability to protect critical infrastructure inside their borders is reason for concern.

FIGURE 2. INTERNET USERS BY LEVEL OF DEVELOPMENT[1], 2006-2011.



1 The classification of countries as developed or developing has been taken from the UN M49 standard.

FIGURE 3. INTERNET USERS PER 100 INHABITANTS, 2001-2011 [3]



But even more worrisome than the possibility of a cyber attack against critical infrastructures is that the Internet itself, we believe, has become a critical infrastructure of sorts. Somewhere in the rapid process of Internet development, some countries have become dependent on the Internet for providing a myriad of their services, such as e-government services, online banking, health services, life-saving instructions, and messages to the public.

This paper examines the Internet as a critical infrastructure, discusses levels of Internet connectivity and the provision of Internet-based services as meaningful indicators of the Internet as a critical infrastructure, and proposes a new framework for measuring countries' susceptibility to cyber attacks.

2. CYBER-ATTACK SUSCEPTIBILITY (CAS) INDEX

The cyber-attack susceptibility (CAS) index, as proposed by the authors of this paper, is composed of four indicators that help one gauge the level of Internet development in a country:

- The percentage of a country's population that uses the Internet. This indicator is based on figures from ITU (International Telecommunications Union) and other online sources [4].
- Online service index. The *United Nations E-Government Survey 2010* explains that "to arrive at a set of online service index values, the UN's research team assessed each country's national website as well as the websites of the ministries of education, labour, social services, health and finance….Among other things, the national sites were tested for a minimal level of Web content accessibility" [5].
- Telecommunication infrastructure index. This index is defined as "a composite of five indicators: number of personal computers per 100 persons, number of Internet users per 100 persons, number of telephone lines per 100 persons, number of mobile cellular subscriptions per 100 persons and number of fixed broadband subscribers per 100 persons" [5].
- Human capital index. The *United Nations E-Government Survey 2010* describes this index as "a composite of two indicators: adult literacy rate and the combined primary, secondary, and tertiary gross enrollment ratio" [5].

The online service index, telecommunication infrastructure index, and human capital index are used in the formula for the United Nations e-government development index (EGDI) [5]:

$$EGDI = (0.34 \bullet \text{online service index}) + (0.33 \bullet \text{telecom.infra.index}) + (0.33 \bullet \text{human capital index})$$

The CAS index score is the mean of the EGDI and the percentage of a country's population that is connected to the Internet:

$$\text{CAS index} = \frac{EGDI + \%\ \text{of population connected to Internet}}{2}$$

The four indicators (the percentage of a country's population that uses the Internet, the online service index, the telecommunication infrastructure index, and the human capital index) together give an idea of the degree to which a country's public participates in the Internet, the level of the country's governmental investment in Internet infrastructure and the technological literacy of the people, and the level of service that the country provides online. In other words, these indicators show the level of a country's Internet development and the reliance of its populace on Internet services.

The downside of a high level of connectivity and online services is that the latter are targets of cyber attacks. By this reasoning, countries that have a high CAS score are more susceptible to an attack that can leave the populace with a degraded Internet connection or none at all and that can result in a state of denial of service, the manipulation of content, or the theft of sensitive data.

3. CAS SCORES BY REGION

Table I lists the CAS scores by region and, in each region, the countries with the highest scores and the countries with the lowest scores.

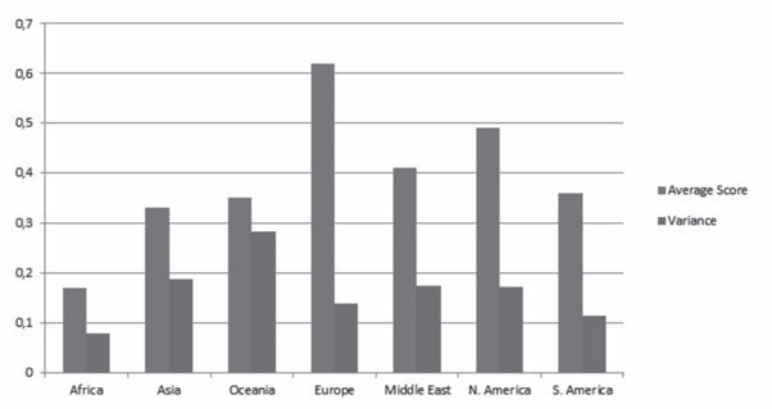
TABLE I: CAS SCORES BY REGION

Region	Mean CAS Score	Variance	Highest-Scoring Countries	Lowest-Scoring Countries
Africa	0.17	0.079	Tunisia, Mauritius	Chad, Niger
Asia	0.33	0.188	Rep. of Korea, Singapore	Nepal, Afghanistan
Oceania	0.35	0.283	Australia, New Zealand	Timor-Leste, Papua New Guinea
Europe	0.62	0.138	Norway, Netherlands	Albania, Bosnia and Herzegovina
Middle East	0.41	0.175	Israel, United Arab Emirates	Yemen, Iraq
N. America	0.49	0.171	United States, Canada	Haiti, Cuba
S. America	0.36	0.114	Argentina, Chile	Suriname, Nicaragua

Not surprisingly, as can be seen in Table I and Figure 4, the regions that have the highest

values for the CAS index are North America and Europe, the birthplace of the Internet. North Americans, especially in the United States and Canada, have become accustomed to the ongoing use of online information and have become reliant on the steady flow of information and services accessed via the Internet. North America's score is lower than Europe's only because of countries such as Cuba and Haiti, which are not as developed as the rest of North America; these countries also come into play in North America's higher variance of CAS scores.

FIGURE 4. CAS SCORES AND VARIANCE BY REGION



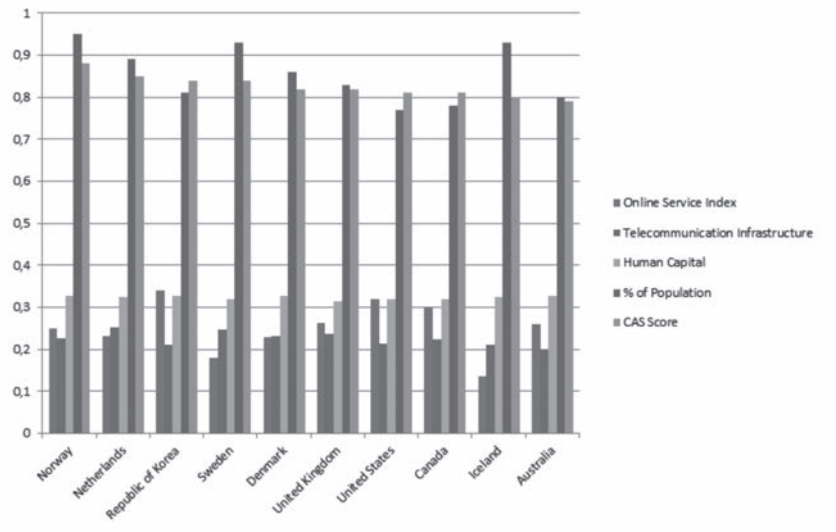
Again not unexpectedly, Africa boasts the lowest CAS score but also has a very low variance, indicating that the entire continent has relatively few online services and low rates of Internet connection and as such relies less on computers and Internet-based communication for everyday tasks and critical infrastructures.

Perhaps the most interesting region is Asia: one Asian country is among the 10 countries with the highest CAS index scores (Table II and Figure 5), but some of the countries that are the lowest CAS scorers are also in Asia (Table I). These two extremes result in a very high variance value (0.188) but can perhaps also affect the ability of Asian countries to cooperate as a region in the combating and mitigation of cyber threats.

TABLE II: TOP CAS-SCORING COUNTRIES AND THEIR COMPONENT INDEXES

Country	Online Services	Telecommunication Infrastructure	Human Capital	% of Population Connected to Internet	CAS Score
Norway	0.2504	0.2254	0.3262	0.95	0.88
Netherlands	0.231	0.253	0.3257	0.89	0.85
Republic of Korea	0.34	0.2109	0.3277	0.81	0.84
Sweden	0.1792	0.2482	0.32	0.93	0.84
Denmark	0.2288	0.2306	0.3278	0.86	0.82
United Kingdom	0.2634	0.2364	0.3149	0.83	0.82
United States	0.3184	0.2128	0.3198	0.77	0.81
Canada	0.3001	0.2244	0.3204	0.78	0.81
Iceland	0.1349	0.211	0.3238	0.93	0.80
Australia	0.2601	0.1983	0.3278	0.80	0.79

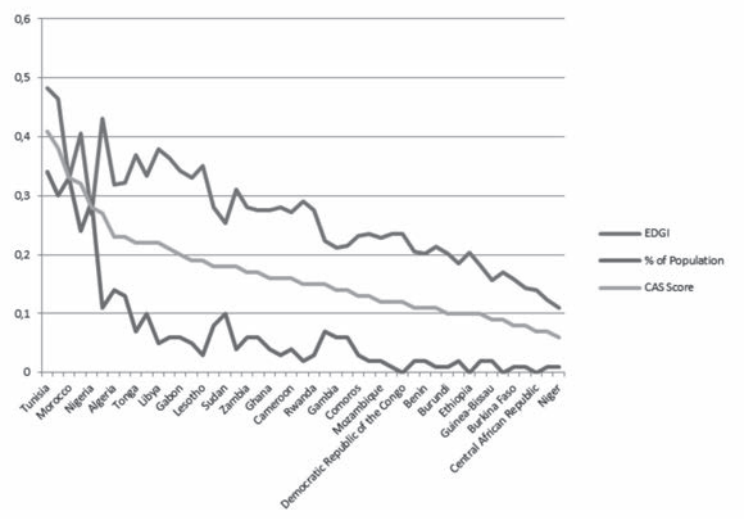
FIGURE 5. TOP CAS-SCORING COUNTRIES SHOWN WITH THEIR COMPONENT INDEXES



4. BREAKDOWN OF CAS SCORES WITHIN EACH REGION[2]

In Africa as a whole, the percentage of the population connected to the Internet is very low (Figure 6). Because the connection rate is below 10 percent for the majority of the countries in Africa, the EGDI is the most influential component of the CAS score for Africa. The CAS scores imply that African countries are not at high risk of cyber attacks.

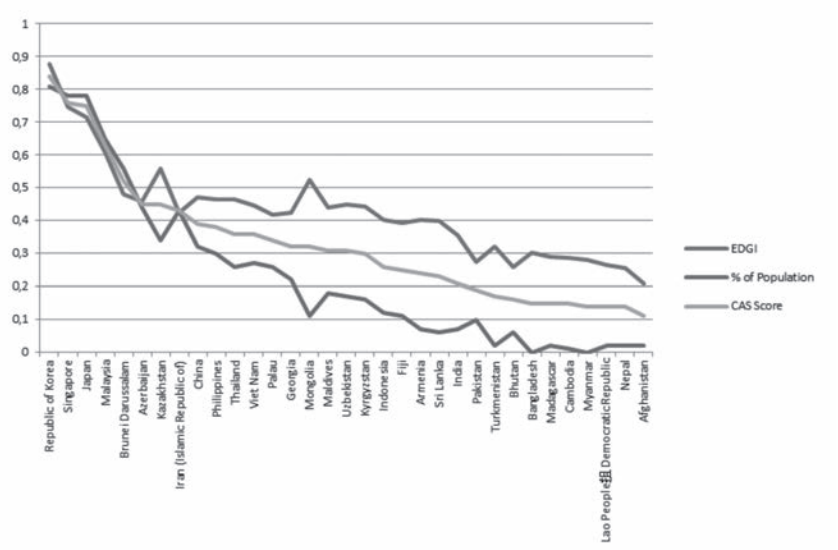
FIGURE 6. CAS SCORES IN AFRICA



2 For the actual CAS index scores of all the countries listed in this section, see the appendix. 6 Council of Europe. 2001. *Council of Europe - ETS No. 185 - Convention on Cybercrime*, [Online]. Available: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

Asia is defined by a very large gap between the countries with the top four scores (the Republic of Korea, Singapore, Japan, and Malaysia) and the rest of the countries in the region (Figure 7).

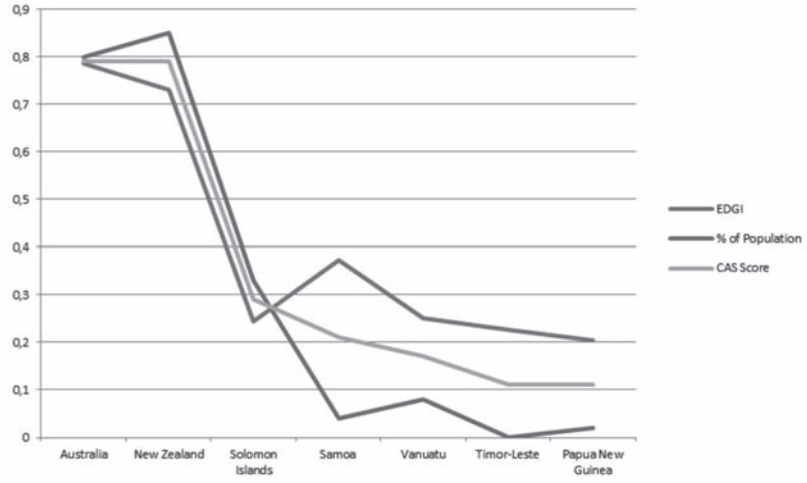
FIGURE 7. CAS SCORES IN ASIA



Cyber attacks are not only a greater threat in the top four countries of Asia, but these countries also have some of the most extensive programs in the world to deal with cyber threats, whereas the rest of the region is not as well positioned to handle such threats.

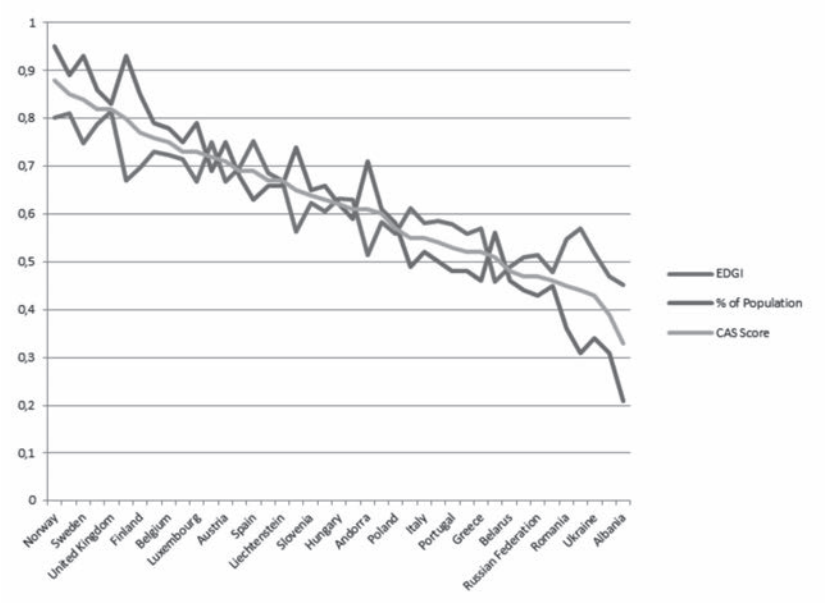
The situation in Oceania is similar to that in Asia: the top two countries (Australia and New Zealand) are much more advanced in Internet connectivity and online services than the rest of the region (Figure 8).

FIGURE 8. CAS SCORES IN OCEANIA



Europe has relatively high CAS scores across the region (Figure 9). There is a clear distinction between the northern part of Europe, which includes Scandinavia and western European countries such as Germany, the United Kingdom, and France and occupies the upper part of the CAS score table, and the southern and eastern parts of Europe, which occupy lower positions in the table.

FIGURE 9. CAS SCORES IN EUROPE

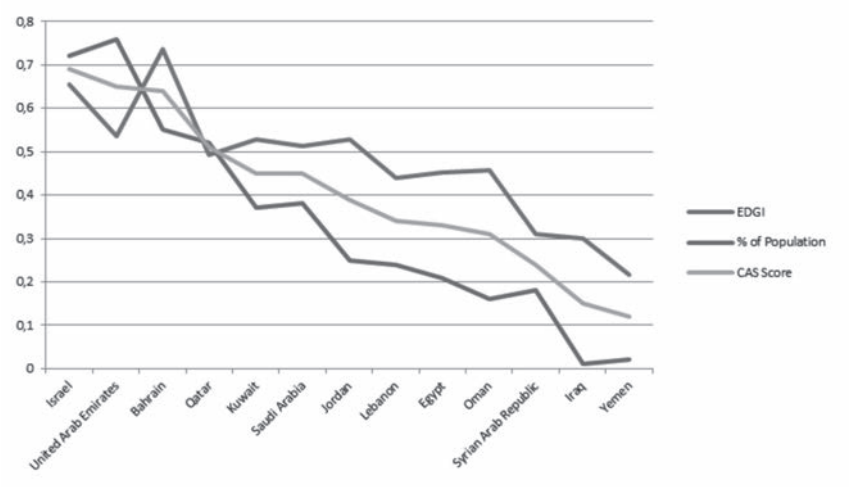


All in all, the comparatively even spread of the CAS scores in Europe enables European countries to more easily arrive at a better understanding regarding cyber threats and build regional structures, such as ENISA[3] (the European Network and Information Security Agency) and the Council of Europe Convention on Cybercrime [6], for facilitating cooperation and collaboration in the cyber sphere.

The scores of the countries in the Middle East demonstrate a clear division between the Persian Gulf States, Saudi Arabia, and Israel, on the one hand, and the rest of the region's countries, on the other (Figure 10).

3 http://www.enisa.europa.eu/

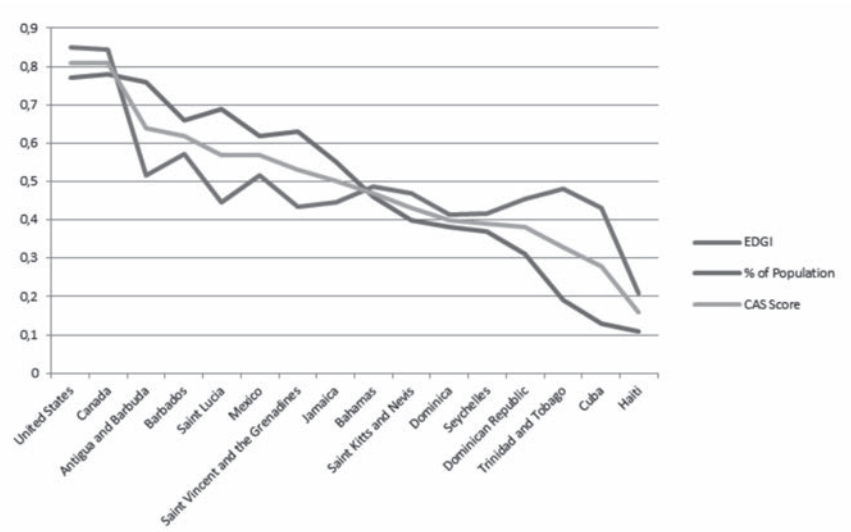
FIGURE 10. CAS SCORES IN THE MIDDLE EAST



Except for Israel, the United Arab Emirates, and Qatar, the CAS scores are influenced more by the EGDI scores than by the percentage of the population that is connected to the Internet, as clearly exemplified by Bahrain. These scores indicate that fewer people are connected to the Internet but the level of service that they obtain is quite good.

North America, like Asia, boasts a wide range of CAS scores (~0.2-~0.8), but unlike the graph for Asia, the North American curve slopes at a relatively steady rate (Figure 11).

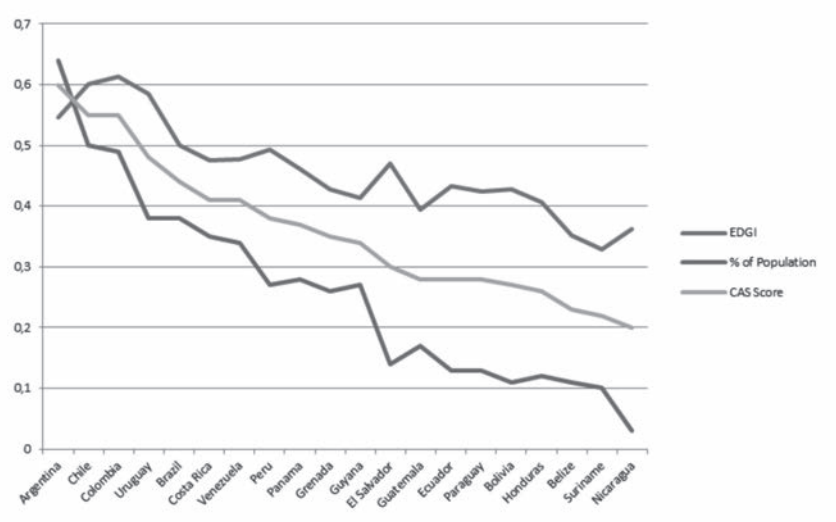
FIGURE 11. CAS SCORES IN NORTH AMERICA



Canada and the United States are the most dominant countries in the region and are also dominant globally. Both exhibit very high EGDI scores and a high percentage of the population connected to the Internet.

Other than Africa, South America is the least connected region in the world, with a very low percentage of the population connected to the Internet (Figure 12). However, the slope of the South American EGDI curve is unusually mild; there is only a small difference between the value for the country with the lowest EGDI score (Suriname) and the value for the country with the highest EGDI score (Colombia).

FIGURE 12. CAS SCORES IN SOUTH AMERICA



5. OVERVIEW OF CIP SCHEMES IN HIGH CAS-SCORING COUNTRIES

In this section, we review the critical-infrastructure protection (CIP) schemes of the seven countries with the highest CAS scores to demonstrate how countries that are at high risk of cyber attacks deal with such threats.

A. Norway

In Norway, the Ministry of Justice has overall responsibility for critical-infrastructure protection [7], with NorCERT as a supporting function for incident response. The Norwegian CIP commission's report identifies two types of systems to be protected. The first—critical infrastructure—includes "electrical power, electronic communication, water supply and sewage, transport, oil and gas, and satellite communication" [8]. The second covers "critical societal functions," which include "banking and finance, food supply, health services, social

services and social security benefit, the Police, emergency and rescue services, [and] crisis management" [8]. The report also indicates additional critical societal functions—"Parliament and government, the judiciary, Defence, Environmental surveillance and waste treatment" [8]—which were not examined by the commission.

B. The Netherlands

In 2005, the government of the Netherlands conducted a risk analysis that demonstrated the need to increase the protection of critical infrastructure [9]. As a result, the National Advisory Center on Critical Infrastructure (NAVI) was formed. With the establishment of the Center for the Protection of Critical National Information Infrastructure (CPNI.nl), NAVI's roles and responsibilities were transferred to that organization. Currently, critical infrastructure in the Netherlands is divided into twelve sectors: energy, telecommunications and ICT, drinking water, food, health, finance, surface water management, public order and safety, legal order, public administration, transport, and the chemical and nuclear industries [10].

C. Republic of Korea

Korea passed the Act on Information and Communications Infrastructure Protection in 2001 to establish a framework for the protection of highly sensitive networks in the country [11]. The supervision of critical-infrastructure protection is conducted by the Information and Communication Infrastructure Protection committee [12], which guides the various government ministries and agencies that handle the day-to-day protection of the critical infrastructure within their purview.

D. Sweden

According to a study by Germany's Federal Office for Information Security (BSI), Sweden's "critical infrastructure protection has been integrated into the general complex of national defense. Critical infrastructure protection is viewed as a combination of information assurance, critical infrastructure protection, defensive information operations and defensive information warfare" [13]. Instead of establishing one organization to be in charge of critical infrastructure protection, Sweden has divided the responsibilities among the Swedish Emergency Management Agency (SEMA), the Technical Competence Centre (TCC), and GovCERT.

E. Denmark

Denmark handles critical infrastructure through two bodies, the Danish Emergency Management Agency (DEMA) and GovCERT [14]. DEMA conducts risk analysis on an ongoing basis, and GovCERT, which belongs to the Ministry of Defence, is in charge of incident response assistance to selected critical-infrastructure owners [15].

F. United Kingdom

On February 1, 2007, the UK formed the Centre for the Protection of National Infrastructure (CPNI) from a merger of the National Infrastructure Security Co-ordination Centre (NISCC) and the National Security Advice Centre (NSAC). CPNI is responsible for providing "integrated security advice […] to organizations which make up the national infrastructure" [16]. CPNI is in charge of the protection of nine national infrastructure sectors: communications, emergency services, energy, finance, food, government, health, transport, and water.

G. United States

The United States has had a broad critical-infrastructure protection scheme in place since 1996. The protection plan was restructured under the Department of Homeland Security (DHS), as specified in the Homeland Security Presidential Directive no. 7 (HSDP-7) in 2003. Each of the protected sectors is under a sector-specific agency, and each agency has established a policy that addresses the various issues of the sector. The sectors that are under protection are agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; the defense industrial base; education facilities; emergency services; energy; healthcare and public health; information technology; national monuments and icons; nuclear reactors, materials, and waste; transportation systems; and water.

6. THE CAS INDEX "TIPPING POINT" MODEL

It is our opinion that by using the CAS index, one can construct a model that indicates the "tipping point"—the point at which nations realize that they are susceptible to a critical threat of cyber attacks. A quick survey of the data presented earlier makes clear that no country with a CAS index below 0.21 has a scheme in place for critical-infrastructure protection. The country with the lowest CAS score that has a well-structured critical-infrastructure plan is India, which is anomalous because of the low percentage of its population, especially in rural areas, that is connected to the Internet (7 percent nationwide). On the other hand, all of the countries with a CAS score above 0.61 boast a working plan for critical-infrastructure protection, with Andorra as the first country without such a plan. Because of its size, Andorra might not need a comprehensive plan to combat cyber threats. The next country in the list without a critical-infrastructure protection plan is the Bahamas, with a score of 0.47, bringing us much closer to India's 0.21 score.

7. CONCLUSIONS

As the data show, the use of the Internet and technology is spreading across the globe. Developing countries are among the nations that are increasing their Internet connectivity at the fastest rates in the world. Along with technological advancement and Internet connectivity comes the threat of cyber attacks against critical infrastructure and hence the need for a framework to measure the susceptibility of countries to cyber attacks.

The CAS index framework can be used for numerous applications, from research to commercial to defense purposes, with more to come. In the future, we intend to expand our research to establish a solid mathematical "tipping point" model and hope that other researchers will use this framework for further investigation.

REFERENCES

[1] ITU. 2011. *Global ICT developments, 2001-2011* [Online]. Available: http://www.itu.int/ict/statistics.

[2] ITU. 2011. *Internet users, by level of development (2006-2011)* [Online]. Available: http://www.itu.int/ict/statistics.

[3] ITU. 2011. *Internet users per 100 inhabitants, 2001-2011* [Online]. Available: http://www.itu.int/ict/statistics.

[4] *World Internet Statistics* [Online]. Available: http://www.internetworldstats.com/stats.htm.

[5] UN Department of Economic and Social Affairs, *United Nations E-Government Survey 2010*, United Nations, New York, 2010.

[6] Council of Europe. 2001. *Council of Europe - ETS No. 185 - Convention on Cybercrime*, [Online]. Available: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

[7] European Network and Information Security Agency, *Norway Country Report*, 2010.

[8] Norway Ministry of Justice, *Protection of critical infrastructures and critical societal functions in Norway*, 2006.

[9] European Network and Information Security Agency, *Netherlands Country Report*, 2010.

[10] Government of Netherlands. 2011. *Protecting Critical Infrasturcture*," [Online]. Available: http://www.government.nl/issues/crisis-national-security-and-terrorism/protecting-critical-infrastructure.

[11] Government of Korea. 2001. *Act on Promotion of Information and Communication Network Utilization and Information Protection* [Online]. Available: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf.

[12] J. Jang, *The Current situation and Countermeasures to Cybercrime and Cyber-Terror in the Republic of Korea*.

[13] BSI. 2004. *Critical Infrastructure Protection: Survey of World Activity* [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.pdf?__blob=publicationFile.

[14] European Network and Information Security Agency, *Denmark Country Report*, 2011.

[15] Centre for the Protection of National Infrastructure. 2012. *The national infrastructure [Online]. Available:* http://www.cpni.gov.uk/about/cni

[16] GovCERT. 2011. *The following profile of the Danish GovCERT has been established in adherence to RFC-2350* [Online]. Available: https://www.govcert.dk/gcdata/rfc2350_govcert.pdf.