The Global Cyber-Vulnerability Report (in-brief)

V.S. Subrahmanian, UMD
M. Ovelgonne, UMD
T. Dumitras, UMD
B.A. Prakash, Virginia Tech

Study Statistics

2	years of data from Symantec
4M+	machines studied per year
20B+	malware/telemetry reports
44	countries

Paradox of Public Awareness

"The more secured a country is, the more vulnerable it is conceived to be by the public. That is because high level of cybersecurity implies high rate of malware detection and, therefore, greater image of vulnerability."

Gen. (Ret.) Isaac Ben-Israel, Founder – Israel National Cyber Bureau, writing in the foreword to the book

Headlines

Despite the widespread perception that the United States is the biggest target for cyber-criminals and nation states, the Global Cyber-Vulnerability Report, published by Springer (Dec. 2015) shows that this is not the case.

Perhaps surprisingly, the countries at greatest risk are South Korea, India, Saudi Arabia, China, Malaysia and Russia. India and South Korea vie for the honor of being considered the most cyber-vulnerable nation in our study. In 2010, 82.7% of Indian hosts were attacked with 17.9 attacks per host on average. During the same year, the corresponding numbers for S. Korea were 81.9% and 15.2 attacks per host. In 2011, the countries switched order, with 91.3% of hosts in S. Korea being attacked by 21.6 attacks per host on average – the corresponding numbers for India in 2011 were 80.9% and 19.5 attacks per host.

Norway and Denmark tied for the honor of being the safest countries in the world from a cybersecurity perspective with 43.7% of Norwegian hosts infected with just 2.87 attacks per host in 2010 – the corresponding numbers for Denmark were 40% and 3.07. In 2011, both nations improved with just 36.4% of Norwegian hosts being attacked with 2.2 attacks per host on average – the corresponding 2011 numbers for Denmark were 35.8% and 2.28 attacks per host. In safety, these countries were followed by Finland, Sweden, and Switzerland. Japan and Germany also did well.

In both years, the USA was ranked the 10th or 11th safest nation from a cyber-vulnerability perspective (55.5% attacked, 4.9 attacks per host in 2010; 48.5% attacked, 3.5 attacks per host in 2011).

Cyber-vulnerability of nations is negatively correlated with major development indices released by UNDP.

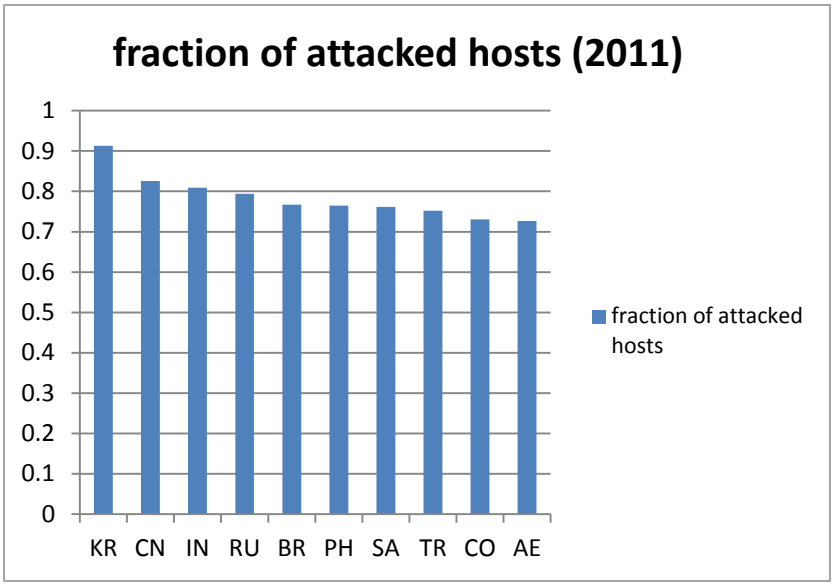
- Per capita GDP
- Human Development Index
- Health Index and Education Index

V.S. Subrahmanian, Michael Ovelgonne, Tudor Dumitras, B. Aditya Prakash, *The Global Cyber-Vulnerability Report*, Springer, Dec 2015. http://www.springer.com/us/book/9783319257587

10 Most Cyber-Vulnerable Countries

South Korea and India tie for being the most cyber-vulnerable countries in the world, with China, Malaysia, Saudi Arabia and Russia close behind.

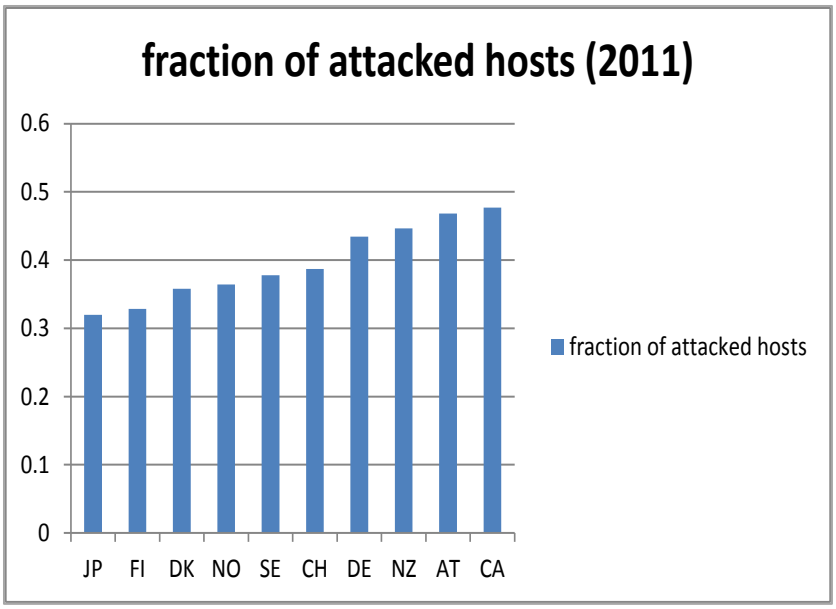
Scandinavian countries are amongst the most cyber-secure nations on earth.



Though India and South Korea vie for being the most cyber-vulnerable nations, China, Russia, Saudi Arabia, and Malaysia are not far behind. For instance, in 2010, 82.5% of Chinese hosts were attacked (more than any other nation) but with only 11.63 attacks per host on average compared to 21.6 in the case of South Korea. *Note: Our study only covered 44 countries and did not include many developing/emerging economies.*

12 Most Cyber-Secure Nations

The most cyber-vulnerable countries in our study.



Common National Cyber Policies

Most of the 44 countries studied have a clear national cybersecurity policy.

Governance structure for cybersecurity varies from country to country. Some countries have a centralized authority (e.g. Israel). In others, responsibility to secure cyberspace devolves to different ministries. Despite the existence of inter-ministry coordinating structures, it is likely that in such cases, threat intelligence will not be properly shared and responses will not be speedily and properly coordinated.

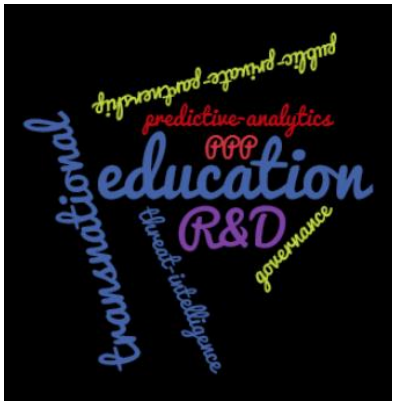
All countries recognize the transnational nature of cybersecurity issues.

All countries recognize the need for public private partnerships involving government, business, and academia.

All countries recognize the value of cybersecurity education and R&D. Yet few have a coherent strategy to achieve this.

Almost no country recognized the risks posed by the Internet of Things and the possibility of air-gapped attacks in their national cybersecurity strategy.

Almost no countries recognize the need to understand what drives their adversary and develop predictive analytic models for cyber-attacks.



Education, R&D, public-private partnerships, governance, as well as transnational partnerships will be key factors in cybersecurity policies.

Cybersecurity Policy Recommendations

Education about cyber-hygiene from the pre-school level up is critical. Countries need to increase funding to schools and universities to improve cyber-education.

Cyber-security professionals in government need salaries that are competitive with industry salaries. Government efforts to recruit cybersecurity experts will need to be fast-tracked.

Countries need to develop systematic processes to identify and respond to attacks.

Countries need to develop systematic methods to track threat intelligence and predict when a cyber-attack will occur.

Legislation and/or regulation is needed to require organizations to report certain types of cyber-events to a centralized authority.

Related Research

Understanding user behavior linked to cyber-vulnerability.

Predicting how a specific piece of malware will spread through hosts in a country.

Identifying how system managers should patch their software, given limited resources.

Optimally allocating security officers to monitor alerts.

Deceiving the attacker.

UNIVERSITY OF MARYLAND

VirginiaTech 1872 Invent the Future

CDIG CENTER for DIGITAL INTERNATIONAL GOVERNMENT

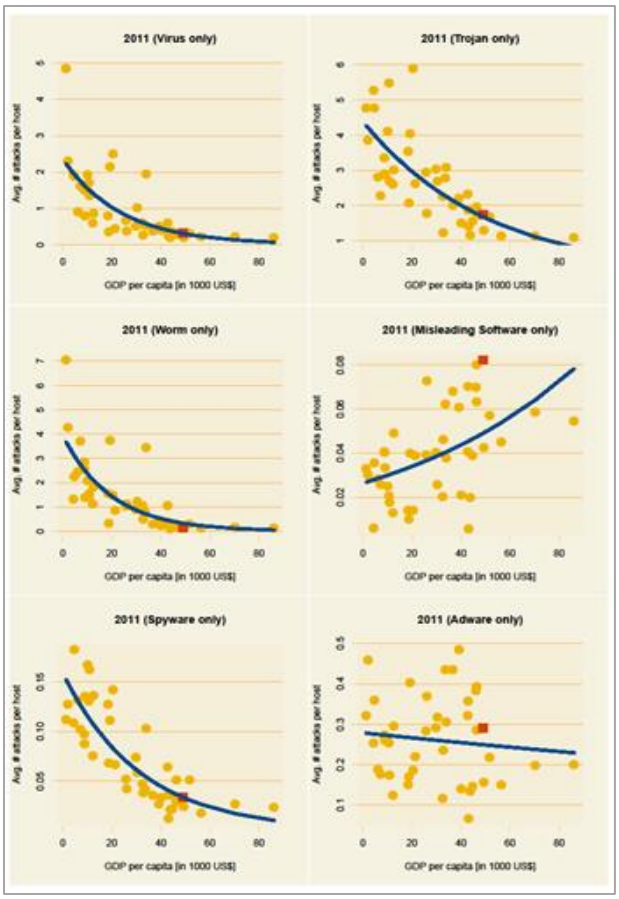
V.S. Subrahmanian, Michael Ovelgonne, Tudor Dumitras, B. Aditya Prakash, *The Global Cyber-Vulnerability Report*, Springer, Dec 2015. http://www.springer.com/us/book/9783319257587

Case Study: USA

Though many reports assert that the USA is the most heavily attacked nation in the world, these reports do not consider the Paradox of Public Awareness and the fact that in the 44 countries we studied, the number of hosts in the US that are monitored by anti-virus engines and security programs was 3-440 times the number in the other 43 countries. *In fact, this suggests that US hosts are much more effectively protected than hosts in other countries.*

Based on our data, the US is around the 10th or 11th safest country on earth from a cyber-security perspective.

The principal threat to hosts in the US is from Trojans, followed by viruses and worms. However, misleading software (such as fake anti-virus programs, fake disk cleanup utilities are far more prevalent in the US compared to other nations with a similar GDP. This suggests that education to recognize and avoid misleading software will be key to US efforts in reducing cyber-threat.



Contact Information

Please contact the study's principal author, Prof. V.S. Subrahmanian, for further information.

Email	vs@cs.umd.edu
Phone	301-405-6724
Twitter	@vssubrah
URL	www.cs.umd.edu/~vs/
Address	Dept. of Computer Science AV Williams Building University of Maryland College Park, MD 20742

V.S. Subrahmanian, Michael Ovelgonne, Tudor Dumitras, B. Aditya Prakash, *The Global Cyber-Vulnerability Report*, Springer, Dec 2015. http://www.springer.com/us/book/9783319257587