Nations ranked on their vulnerability to cyberattacks

March 9 2016

Credit: Wikipedia

Damaging cyberattacks on a global scale continue to surface every day. Some nations are better prepared than others to deal with online threats from criminals, terrorists and rogue nations.

Data-mining experts from the University of Maryland and Virginia Tech recently co-authored a book that ranked the vulnerability of 44 nations to cyberattacks. Lead author V.S. Subrahmanian discussed this research on Wednesday, March 9 at a panel discussion hosted by the Foundation for Defense of Democracies in Washington, D.C.

The United States ranked 11th safest, while several Scandinavian countries (Denmark, Norway and Finland) ranked the safest. China, India, Russia, Saudi Arabia and South Korea ranked among the most vulnerable.

"Our goal was to characterize how vulnerable different countries were, identify their current cybersecurity policies and determine how those policies might need to change in response to this new information," said Subrahmanian, a UMD professor of computer science with an appointment in the University of Maryland Institute for Advanced Computer Studies (UMIACS).

The book's authors conducted a two-year study that analyzed more than 20 billion automatically generated reports, collected from 4 million machines per year worldwide. The researchers based their rankings, in part, on the number of machines attacked in a given country and the number of times each machine was attacked.

Machines using Symantec anti-virus software automatically generated these reports, but only when a machine's user opted in to provide the data.

Trojans, followed by viruses and worms, posed the principal threats to

machines in the United States. However, misleading software (i.e., fake anti-virus programs and disk cleanup utilities) is far more prevalent in the U.S. compared with other nations that have a similar gross domestic product. These results suggest that U.S. efforts to reduce cyberthreats should focus on education to recognize and avoid misleading software.

In a foreword to the book, Isaac Ben-Israel, chair of the Israeli Space Agency and former head of that nation's National Cyber Bureau, wrote: "People—even experts—often have gross misconceptions about the relative vulnerability [to cyber attack] of certain countries. The authors of this book succeed in empirically refuting many of those wrong beliefs."

The book's findings include economic and educational data gathered by UMD's Center for Digital International Government, for which Subrahmanian serves as director. The researchers integrated all of the data to help shape specific policy recommendations for each of the countries studied, including strategic investments in education, research and public-private partnerships.

Subrahmanian's co-authors on the book are Michael Ovelgönne, a former UMIACS postdoctoral researcher; Tudor Dumitras, an assistant professor of electrical and computer engineering in the Maryland Cybersecurity Center; and B. Aditya Prakash, an assistant professor of computer science at Virginia Tech.

A related research paper on forecasting the spread of malware in 40 countries—containing much of the same data used for the book—was presented at the 9th ACM International Conference of Web Search and Data Mining in February 2016.

Another paper, accepted for publication in the journal *ACM Transactions on Intelligent Systems and Technology*, looked at the human

aspect of cyberattacks—for example, why some people's online behavior makes them more vulnerable to malware that masquerades as legitimate software.

Provided by University of Maryland