View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Institutional Knowledge at Singapore Management University

Singapore Management University

Institutional Knowledge at Singapore Management University

Research Collection School Of Information Systems

School of Information Systems

3-2012

A Comparative Study of Cyberattacks

Seung Hyun KIM

QIU-HONG WANG
Singapore Management University, qiuhongwang@smu.edu.sg

Johannes B. ULLRICH

DOI: https://doi.org/10.1145/2093548.2093568

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

Part of the Information Security Commons

Citation

KIM, Seung Hyun; QIU-HONG WANG; and ULLRICH, Johannes B.. A Comparative Study of Cyberattacks. (2012). *Communications- ACM*. 55, (3), 66-73. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/3222

This Journal Article is brought to you for free and open access by the School of Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email libIR@smu.edu.sg.

A Comparative Study of Cyberattacks

By Seung Hyun Kim, Qiu-Hong Wang, Johannes B. Ullrich

Published in Communications of the ACM, 2012 March, Vol. 55 No. 3, Pages 66-73.
http://dx.doi.org/10.1145/2093548.2093568

Cyberattacks are computer-to-computer attacks undermining the confidentiality, integrity, and/or availability of computers and/or the information they hold.[a] The importance of securing cyberspace is increasing, along with the sophistication and potential significance of the results of the attacks. Moreover, attacks[b] involve increasingly sophisticated coordination among multiple hackers across international boundaries, where the aim has shifted from fun and self-satisfaction to financial or military gain, with clear and self-reinforcing motivation; for example, the number of new malicious code threats worldwide increased more than 71% from 2008 to 2009. [14]

Key Insights
The worldwide effort to safeguard against attacks seems to lack coordination and collaboration. The majority of cybercriminals go unpunished, with their skills often exceeding those of the international authorities responsible for stopping them. [8] One economic barrier to information security is the presence of “externalities” [1]; an example of a negative externality is when a computer infected by a virus harms other computers in the same network, and a positive externality is when a security breach targeting specific software with a large installed base is disclosed, possibly alerting other users and preventing further loss due to being attacked. In economics, positive externalities drive economic agents to invest less than would be socially desirable, even when protection is technically feasible. Among countries, one country's effort in terms of enforcement and investment in security infrastructure makes other countries more secure by reducing the number of attacks originating from within its borders. Alternatively, attackers who are themselves threatened may virtually relocate to other countries. Such externalities inhibit achievement of a globally desirable level of country-level investment and enforcement action.

Information security is recognized as both a technical issue and a critical policy and business issue.[10] The presence of externalities in information security scenarios requires international collaboration among national governments.[7] The Convention on Cybercrime (Europe Treaty Series No. 185)[c] adopted by the Council of Europe, November 23, 2001, was the first and is still the most important international treaty focused on cybercrimes, aiming to “set up a fast and effective regime of international cooperation.”[d] As of January 2012, 32 countries have ratified the Convention, though 17 member countries have not.[e] Li wrote, “The pressure against not ratifying the treaty coming from inside the countries seems to be a greater obstacle than the differences over the drafting of the document.”[5]

[a] Based on *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: GAP Analysis Report*. Institute for Security Technology Studies, Dartmouth College, 2004;http://www.ists.dartmouth.edu/projects/archives/gar.html
[b] Hackers are defined as violators of information security; in this study, attackers and hackers were viewed as equivalent.
[c] We say "the Convention" as shorthand for the Convention on Cybercrime (European Treaty Series No. 185).
[d] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
[e] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

The first step toward improving international collaboration is to understand the nature of the attacks, with respect to national demographics and international policy. For instance, cybersecurity research by ISPs has sought to identify organizations hosting abnormally high levels of malicious content.[4,13] While industry-based research and recommendations on information security (such as *Symantec Internet Security Threat Reports* and *Microsoft Security Intelligence Reports*) are publicly accessible, they tend to focus on the technical aspect of cyberattacks rather than on their effects on policy and business. Therefore, more information about countries hosting malicious activity is required, including how attacks are distributed and correlated among them, and how these security statistics link to national demographics and international policy.

This article explores the nature and scope of cyberattacks originating from a number of countries, analyzing SANS Institute country-level intrusion-detection samples, 2005–2009. The SANS Institute established the Internet Storm Center (ISC http://isc.sans.edu/) in 2001, aiming to assist ISPs and end users to safeguard themselves against cyberattacks. The ISC monitors the kind of data-collection, analysis, and warning systems used in weather forecasting. The DShield data set used by ISC is a collection of network-security logs from its voluntary subscriber base throughout the Internet. Each DShield contributor reports information about the source of an attack whenever an alert is sounded by its firewall. Given its worldwide coverage, the DShield dataset provides a relatively accurate representation of malicious traffic, as detected by hundreds of networks.[12] Though the logs are not comprehensive enough to fully disclose specific types of attacks and the location of the original attacker(s), it does show the aggregate selection of sources from where the attacks might have originated. Following the rational-choice theory in classic criminology,[6] criminals make decisions to maximize their net return by weighing potential costs and benefits. Any country with abundant resources and porous borders is likely to become the sanctuary for cyberattacks; hence, the nature of the DShield dataset fits well with our research interests.

Our analysis of country-level data yielded three important lessons (described in the following sections) that could be a foundation for further collaboration and coordination among countries:

Lesson 1. Identify the top sources of attacks from demographic characteristics. Ranking countries by number of attacks based on the SANS data (see Figure 1) is similar to that published by Symantec Corporation.[14,15] The distribution of cyberattacks skews heavily toward certain countries; the SANS data shows that the top 10 (20) countries accounted for 74.3% (87.3%) of the total number of global attacks in 2009. Thus the top countries may be considered more responsible than other countries for the rampant cyberattacks.

However, the volume of attacks alone cannot be used to identify relative likelihood of threats and guide international collaboration. Logically, the number of cyberattacks originating from any single country is related to development of its information infrastructure, Internet penetration, and domestic population.[5] This correlation leads to the formation of three additional indices of top origin after adjusting for economic development (see Figure 2a), population (Figure 2b), and number of Internet users (Figure 2c), respectively (see Table 1).[f] These indices are useful indicators for identifying threats previously ignored due to being hidden within the enormous volume of attacks. In these indices, the highest-ranking countries in terms of number of originating

[f] Source: Euromonitor International's Global Market Information Database. We excluded countries with relatively few computers (<400,000 in 2005); they also generally have relatively low economic development and would possibly inflate our indices due to their small denominators. Likewise, the samples from these countries in the SANS dataset are less stable than those from other countries.

attacks are encouraged to improve their information-security infrastructure and enhance legal enforcement against attacks, as well as against the heaviest attack generators by volume. We find substantial differences across the three indices, which seem to complement one another. Zimbabwe (ignored in other indices) is identified as the top source of attacks per capita; Estonia, Latvia, and Slovenia are also more important threats than is indicated by attack volume alone.[g] Likewise, the attacks per GDP PPP (purchasing power parity) reveals potential threats from Bulgaria, Costa Rica, Estonia, Jordan, and Latvia, and attacks-per-Internet-user includes Bangladesh and Slovenia.

However, none of these demographic factors alone fully explains the variation in cyberattacks among countries. Hence, we conduct a simple regression to identify additional countries with an inherently large volume of attacks that cannot be explained by standard demographic parameters. The following formula represents a regression model, with each variable representing the ratio over its global level on an annual basis where a residual term equals the observed proportion of attacks minus the proportion predicted by the evaluated parameters and captures the component that cannot be justified by economic development, population, and Internet penetration.[h] Thus, a positive residual indicates attacks beyond expectations originating from a country relative to the global average; a negative residual indicates fewer attacks than expected; the top countries can be identified by residuals, as in Table 1. Table 1 also lists countries among the top 20 by total attack volume, to which the regression model attributes the most overestimated attacks; the residual term is a large negative. These countries might indicate possible overrepresentation when applying the volume-based approach alone. The U.S. is most frequently among the top 10. In addition, most of the top countries (based on total attack volume), except China, have signed or ratified the Convention, including France, the Netherlands, and the U.S., and most countries in which the number of hosted attacks is below the global average have likewise signed or ratified. Among them, the number of attacks originating from France, Japan, and the U.K. was below the global average in the years (2005–2009) we surveyed, despite their considerable economic development, population, and Internet penetration. Canada and Spain, which were both at the top for volume of originating attacks in 2005 with an extraordinary number of attacks, surprisingly generated fewer cyberattacks than the global average in 2009. Moreover, three of the nine overrepresented countries in 2009 in Table 1—Canada, Japan, and Poland—were among the 13 countries that signed the Convention in 2005 (or earlier) but still have not ratified it. Due to the number of attacks below the global average, these countries may not have as much incentive to join as other developed countries. In contrast, some countries with negligible total attack volume were among the top 20, 2005–2009, with an extraordinary number of attacks, including Bangladesh and Zimbabwe. The number of such underrepresented countries increased from two in 2005 to six in 2009, with none signing the Convention.

These observations reflect the international divide and dynamics of attack sources associated with the Convention. First, the top-origin countries, having developed economies, are more likely to accede to the Convention, though they remain sanctuaries of cyberattacks and potential cyberattackers, even after ratification of the Convention, including Germany and the U.S. Second, developing countries that have not ratified the Convention host disproportionately more attacks and potential attackers than would otherwise be projected from their economic

[g] Rankings of these countries changed by 20 or more places compared to their rankings based on attack volume. We chose countries with populations of more than one million to eliminate high rankings due to small denominators; likewise, we excluded countries with GDP PPP <$25 million and number of Internet users <800,000, 2005–2009.

[h] As the three variables correlate with one another, estimates of coefficients are less precise, so are not reported. Despite such correlations, we are better off including these factors to obtain residuals they do not explain; R-squared values for all estimated models are >85%.

development, population, and Internet penetration. Consequently, while the benefit of joining the Convention is not reflected in the top lists of attack origins, there is a spillover effect on countries that have not joined. In fact, such an international divide on international collaboration motivates attackers to launch attacks due to the risk advantage from facilitating worldwide network connectivity. Developing countries have relatively poor information-security infrastructure and insufficient resources for deterring cyberattacks.5 As a result, the lower risk of launching cyberattacks from them may attract attackers seeking sources that leverage the risk advantage.

Overall, the combination of total attack volume and demographic characteristics reveals inherently high threat levels of cyberattacks in certain countries, partly negating responsibility of countries that may be overrepresented in terms of total attack volume.

Lesson 2. Global diffusion trend across regions, not countries. The world has flattened across regions in terms of sources of cyberattacks. We employed the Herfindahl index to examine this phenomenon, a commonly used measure of industry concentration calculated for any given year by $H = \Sigma Ni\ S2i$, where N denotes the number of countries and Si is the share of country i out of total attacks. Based on the Herfindahl index, Figure 3 reflects a diffusion trend of attacks globally and across regions. The decreasing Herfindahl index indicates the diffusion of attacks across regions, and is consistent with global diffusion. However, global diffusion in cyberattacks did not spread evenly across all countries. Rather, attacks within Asia and Africa have become more concentrated over time, while the Herfindahl index for European countries did not vary from 2005 to 2009. That concentration was led by the surge in share of attacks originating from a few countries (see Table 2). Interestingly, most countries listed in Table 2 have still not ratified the Convention (except Romania and Belgium) and are listed in Table 1 as the top countries with extraordinary attacks in 2009.

The global-diffusion trend across regions, not countries, manifests through manipulation of attack sources by attackers. While the world is highly connected through the Internet, cybercriminal legislation and jurisdiction sometimes stops at national borders. This limited coverage facilitates “risk arbitrage,” with attackers able to commit cyberattacks with relatively low risk of government enforcement by exploiting the divide between domestic legislation and jurisdiction. As a result, attackers expand their attack sources (such as botnets) while focusing on countries with underdeveloped information-security infrastructures.

Lesson 3. Considerable interdependence of global trends and compelling substitution effect. Interdependence represents another major weakness concerning cyberattacks at the country level; we define interdependence as the co-movement of attacks between countries. Positive correlation between cyberattacks originating from two countries represents movement in the same direction, while negative correlation represents movement in opposite directions. Interdependence is measured by the correlation of the weekly global proportions of attacks between any pair of countries. This method helps tease out co-movement in attacks between two countries due to the global trend; for example, our factor analysis found that for the top 16 countries ever listed as a top-10 country for attack origin (2005–2009), 49% of attacks could be explained by a single (general) factor that can be labeled “global co-movement.”[i]

After ruling out the grand global trend, we still observed a high level of positive interdependence between given pairs of countries.[j] The pair-wise correlations (based on volume and proportion of attacks, respectively) between

[i] Vulnerability embedded in a dominant software platform could expose millions of computers to security threats.

[j] Our measure of pairwise interdependence is conservative, as it might underestimate positive interdependence; an increase in one country's share from a surge in attacks originating from within its borders decreases other countries' shares of attacks worldwide, with the denominator becoming greater for all other countries.

the U.S. (a dominant source among countries identified as harboring malicious activity) and other countries (2005–2009) are outlined in Figures 4a and 4b. Using correlation of shares of attacks, the correlation between the U.S. and other countries, as in Figure 4b, dramatically decreased compared to the correlation of attack volume in Figure 4a. In Figure 4b, France is seen as having the highest pair-wise correlation (0.53) with the U.S. Other countries with positive correlations above 0.30 with the U.S. include the Philippines (0.39), Slovenia (0.38), Estonia (0.36), and Singapore (0.35) in descending order of correlation, respectively. We also confirmed positive pair-wise interdependence as stronger among certain countries, including Japan and South Korea (0.65).

Despite considerable global co-movement, as in Figure 4a, Colombia was negatively correlated with the U.S. (-0.40). We found significant negative correlations between the U.S. and several countries, even after adjusting the denominator to reduce possible overestimation of pair-wise interdependence.[k] While Lesson 2 on global diffusion revealed that attack sources might disproportionately concentrate in certain countries, Lesson 3 on interdependence suggests that some attack sources might simultaneously substitute other attack sources.

Positive interdependence in cyberattacks results directly from the most general technique applied in a cyberattack: First, the attacker communicates hacking experience and skills via online forums, helping other attackers exploit software vulnerabilities simultaneously. Second, computers in various locations might be compromised, thus becoming part of a botnet, or zombie network. A botnet consisting of more distributed computers could leverage the economies of scale in operational cost and increase the chance of successful attacks. Thus, attackers (such as botmasters) might initiate attacks from multiple countries by controlling millions of infected computers. Finally, malicious code (such as Trojans and worms) could propagate across networks through Internet traffic, data exchange, and access.

In contrast, negative interdependence in cyberattacks is probably related to the displacement effect identified by Png et al.[9] that the announcement by the U.S. government on enforcement against cybercriminals could indirectly increase the number of attacks originating from other countries. That is, to avoid increased risk of punishment in the U.S., attackers are thus motivated to relocate their botnets from there to other countries with lower risk.

Though specific types of collaboration and countermeasures may differ with respect to positive and negative interdependence, improved international collaboration is essential. Positive interdependence may be reduced through improved implementation of the Convention on Cybercrime, while negative interdependence may require improved country-to-country collaboration to minimize the incentive to shift attacks between countries.

75 Countries

Based on SANS Institute daily reports on country-level intrusion detection (2005–2009), our study applied the economic indices to analysis of the volume of cyberattacks originating from 75 countries, with coverage limited by the availability of data. For example, no observations were reported from countries with DShield contributors,

[k] Overestimation on negative interdependence is due to the same reason as in footnote j; hence, we use the global-attack volume minus the attacks originating from within the U.S. as the denominator to calculate approximate global shares of attacks from all countries other than the U.S., then examine their correlation with the U.S. global share, respectively. The extent of negative correlation between the U.S. and other countries is smaller than before the adjustment but stays at the same level; countries in descending correlation order include Romania (-0.48), Peru (-0.40), Colombia (-0.39), Australia (-0.33), and Denmark (-0.32).

as the DShield dataset was subject to errors and noise due to misconfiguration of network intrusion and detection systems and false reports.[12]

Our analysis of country-level data yielded three important lessons that may provide a foundation for further collaboration and coordination among countries. The diffusion and interdependence trend of cyberattacks (Lessons 2 and 3) (2005–2009) highlights the importance of international cooperation and implementation of policies in fighting cyberattacks. However, the present cooperation in detection, investigation, and prosecution both domestically and internationally, including the Convention, is insufficient for relieving the worldwide threat to information security. This limitation is evidenced by the extraordinary ongoing surge in cyberattacks originating from certain countries and the persistence of attacks from other countries at the top of the list (Lesson 1).

Unfortunately, incentives for countries to join the Convention are limited due to concern over the cost of legal cooperation and invasion of national sovereignty.[5,7] Apart from Canada, Japan, and the U.S., most countries signing the Convention are members of the European Union. Without worldwide agreement, attackers are free to leverage the risk advantage in countries outside the Convention with poor information security infrastructures. These countries (identified by our analysis) represent hidden sources behind the top sources of cyberattack origin based on total attack volume (such as Bangladesh and Columbia).

Unfortunately, incentives for countries to join the Convention are limited due to concern over the cost of legal cooperation and invasion of national sovereignty.

For countries in compliance with the Convention, positive externalities in information security limits incentives to cooperate at the expected level.[7] Thus, it is not strange that Germany, Denmark, and the Netherlands hosted an extraordinary number of attacks, given they fully complied with the Convention (Lesson 1). Furthermore, insufficient effort maintaining information security and enforcement may exacerbate global security threats due to negative externalities.

National Responsibility

Based on this discussion and our observations, we suggest the following steps for national governments worldwide:

Measurement. First, in order to create an effective mechanism to tackle cybercrime, they need precise measurement of cyberattacks originating from each country, something generally missing from any road map on international collaboration. Indeed, such an approach would help address the *ex ante* incentive of international collaboration and ex post incentive of sufficient inputs.

The state of attack deterrence today recasts a well-known principle involving software quality: “You can't control what you can't measure.”[2] Lack of widely accepted, reliable, stable measurement of the number of cyberattacks originating from each country inhibits understanding a particular country's rights and liabilities in relieving the global threat to information security.

The DShield database may provide a feasible baseline to motivate and strengthen international collaboration on information security. We may refer to the global debate on carbon-dioxide emission control, which likewise incorporates the characteristics of externalities. For instance, global carbon-dioxide emissions are effectively controlled by incorporating the infrastructure and economic state of countries with statistical estimates of emissions from multiple organizations.[3,16] In the cyberattack context, a similar "charge" may be issued to each country, depending on responsibility and demographic status.

Responsibility. Second, given the cross-border aspects of cyberattacks, we stress national responsibility of countries that might host compromised computers, possibly involving intermediate cyberattacks launched by foreign perpetrators. Unlike the sources of carbon emissions, which may be traced, measurement of cyberattacks originating from individual countries includes attacks unconsciously hosted by compromised computers in one country while the physical location of hackers is elusive, as reflected in DShield data. In such a case, the country is actually an intermediary facilitating cyberattacks. For instance, the notable increase in malicious-code ranking for Brazil in 2009 compared to previous years was actually due to the Downadup worm infecting a large number of computers in Brazil.[14] As intermediaries bear less responsibility than victims for a loss due to a cyberattack, there is less incentive to avoid becoming an intermediary than a victim. In order to reach an optimal level of investment in global information security, any measurement must take into account the number of cyberattacks passing through a particular country.

Collaboration. Third, based on any available measurement of cyberattacks, the indices we adopted in our study provide further insight when selecting partner countries for regional collaboration. Top countries listed by both "total volume" and "extraordinary number of attacks" represent a much greater threat to global information security than other countries. Their participation is thus crucial to collaborative enforcement, as with Denmark and the U.S. in Table 1. Top countries with surged shares of cyberattacks that might otherwise be ignored due to their negligible volume reflect the movement of underground forces committing cyberattacks, as with Colombia and Romania in Table 2. Finally, the high correlation among groups of countries in cyberattacks may indicate the countries' participation in hacker activity, including zombie networks, and network traffic. Their joint commitment and participation is thus required to deter cybercriminals.

Constitutional conflict. Fourth, as it is difficult to achieve global collaboration in information security quickly, priority must be given to more critical information-security issues and certain developing countries; for example, some provisions in the Convention might conflict with constitutional principles of certain countries. The Convention takes a broad view, including cybercrimes that, though important, are less related to cyber hacking (such as copyright and child pornography) but might run counter to constitutional law. It is permissible for parties to the Convention to modify their obligations on a limited number of the Convention's Articles; for instance, the U.S. has "taken a partial reservation to the Jurisdiction article (Article 22, Jurisdiction) because it does not as a general matter assert jurisdiction over crimes committed by U.S. citizens abroad (see the U.S. Department of Justice home page http://www.justice.gov/)."

It is important to assert which articles and provisions are more critical for cybersecurity against hacking and should be prioritized or strongly mandated. Otherwise, the full benefit of legal harmonization is simply not possible. Regarding prioritization, we identified certain developing countries that generate more attacks disproportionate to their economic development. They may promise higher return on investment in improving the state of global cybersecurity compared to other developing countries but lack sufficient resources and the technical foundation to comply with the standard required by the Convention. The benefit of joining the Convention for these countries is relatively low because their national industrial infrastructure is less dependent on a network economy. For them participation should thus be prioritized with appropriate technical and/or financial support. The Convention has supported multiple projects to guide developing countries but has concentrated on Eastern Europe.

Conclusion

An alternative approach to worldwide cybersecurity beyond these four suggestions is to adopt the view introduced by Schjølberg and Ghernaouti-Hélie[11] that "A Treaty or a set of treaties at the United Nations level on cyber security and cyber crime should be a global proposal for the 2010s that is based on a potential for consensus." [11] The Convention is still viewed by most countries outside Europe as a regional initiative, though full benefit of legal cooperation is possible only when all the countries ratify any treaty in light of the strong interdependence of cyberattacks across countries.

We hope our suggestions trigger a fruitful discussion that enhances the state of international collaboration and legal harmonization.

Acknowledgments

We thank Ivan Png at the National University of Singapore (NUS) for helpful advice and for financial support from the Natural Science Foundation of China (71001042) and the Ministry of Education Academic Research Fund, NUS (R-253-000-089-112). Corresponding author: Qiu-Hong Wang (qhwang@mail.hust.edu.cn).

References

1. Anderson, R. and Moore, T. The economics of information security. *Science 314*, 5799 (Oct. 27, 2006), 610–613.
2. DeMarco, T. *Controlling Software Projects: Management, Measurement, and Estimation*. Yourdon Press, New York, 1982.
3. International Energy Agency. *CO2 Emissions from Fuel Combustion: Highlights*, 2009; http://www.iea.org/co2highlights
4. Kalafut, A., Craig, S., and Gupta, M., Malicious hubs: Detecting abnormally malicious autonomous systems. In *Proceedings of the 29th Conference on Computer Communications* (San Diego, Mar. 15–19, 2010), 1–5.
5. Li, X. International actions against cybercrime: Networking legal systems in the networked crime scene.*Webology 4*, 3 (Sept. 2007); http://www.webology.org/2007/v4n3/a45.html
6. McCarthy, B. New economics of sociological criminology. *Annual Review of Sociology 28* (2002), 417–442.
7. Moore, T., Clayton, R., and Anderson, R. The economics of online crime. *Journal of Economic Perspectives 23,* 3 (Summer 2009), 3–20.
8. Moscaritolo, A. Border crossing: Fighting international cybercrime. *SCMagazine* (Sept. 2009);http://www.scmagazine.com/border-crossing-fighting-international-cybercrime/article/148562/

9. Png, I.P.L., Wang, C.Y., and Wang, Q.H. The deterrent and displacement effects of information security enforcement: International evidence. *Journal of Management Information Systems 25*, 2 (Fall 2008), 125–144.

10. Png, I.P.L. and Wang, Q.H. Information security: Facilitating user precautions vis-à-vis enforcement against attackers. *Journal of Management Information Systems 26*, 2 (Fall 2009), 97–121.

11. Schjølberg, S. and Ghernaouti-Hélie, S. A global treaty on cybersecurity and cybercrime. Cybercrimelaw. net, CybercrimeData AS, Norway, 2011;http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf

12. Soldo, F. *Predicting future attacks*, Technical Report, 2009;http://www.ece.uci.edu/~athina/PAPERS/dshield-analysis-tr.pdf

13. Stone-Gross, B., Kruegel, C., Almeroth, K., Moser A., and Kirda, E. FIRE: FInding Rogue nEtworks. In*Proceedings of the Annual Computer Security Applications Conference* (Honolulu, HI, Dec. 7–11, 2009), 231–240.

14. Symantec Corp. Global Internet Security Threat Report: Trends for 2009, White Paper. Symantec, Mountain View, CA, Apr. 2010; http://www.symantec.com/business/threatreport/archive.jsp

15. Symantec Corp. *Symantec Global Internet Security Threat Report: Trends for July 5-Dec. 5, White Paper*. Symantec, Mountain View, CA, Mar. 2006; http://www.symantec.com/business/threatreport/archive.jsp

16. United Nations. *United Nations Millennium Development Goals Indicators*, 2010;http://mdgs.un.org/unsd/mdg/Data.aspx

Authors

Seung Hyun Kim (kimsh@comp.nus.edu.sg) is an assistant professor in the Department of Information Systems of the National University of Singapore.

Qiu-Hong Wang (qhwang@mail.hust.edu.cn) is an associate professor in the Department of Information Management and Information System, School of Management of the Huazhong University of Science and Technology, China.

Johannes B. Ullrich (jullrich@sans.edu) is chief research officer of The SANS Institute, Bethesda, MD.

Figures

Figure 1. Attack rankings, 2009.

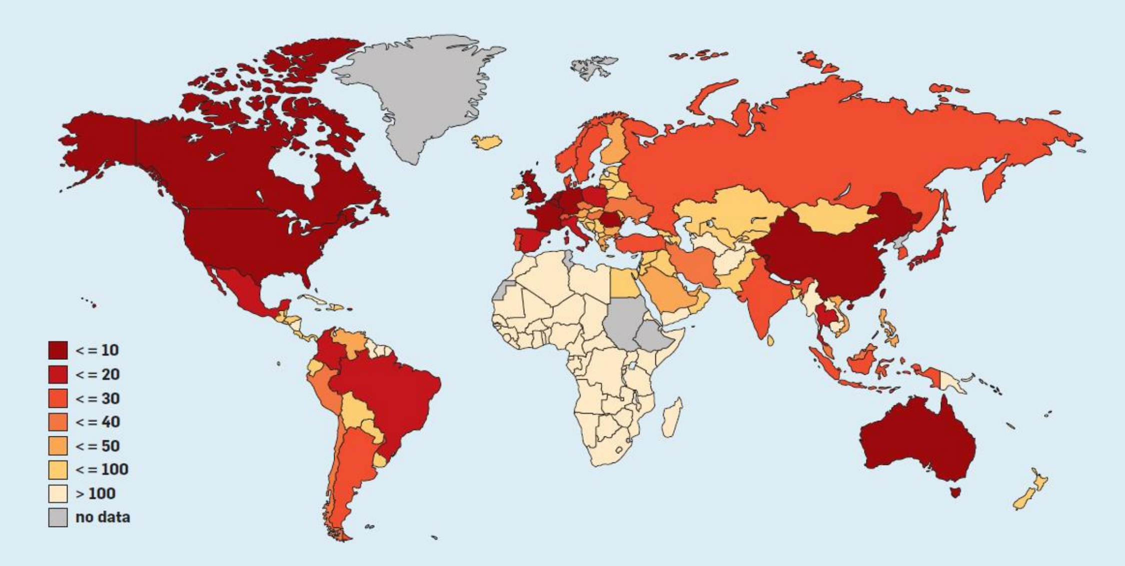


Figure 3. Herfindahl index by year (three-year moving average).

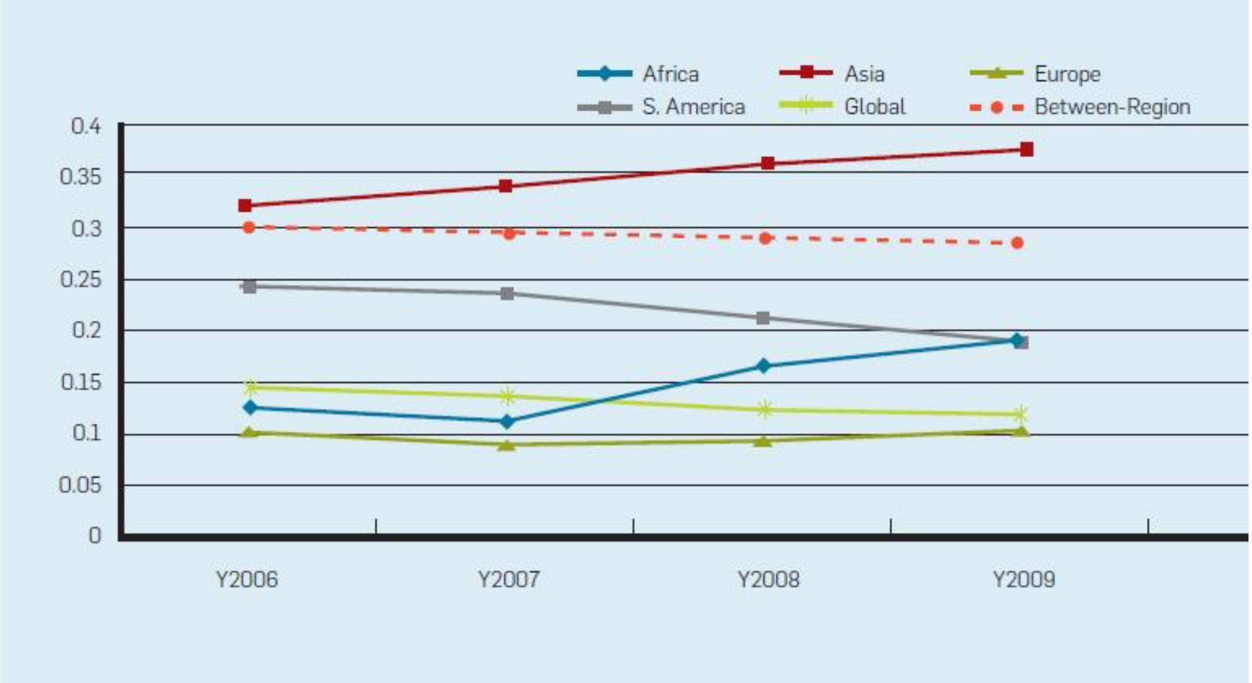


Figure 2. (a) Attack/GDP PPP; (b) attack/population; (c) attack/Internet user rankings, 2009.

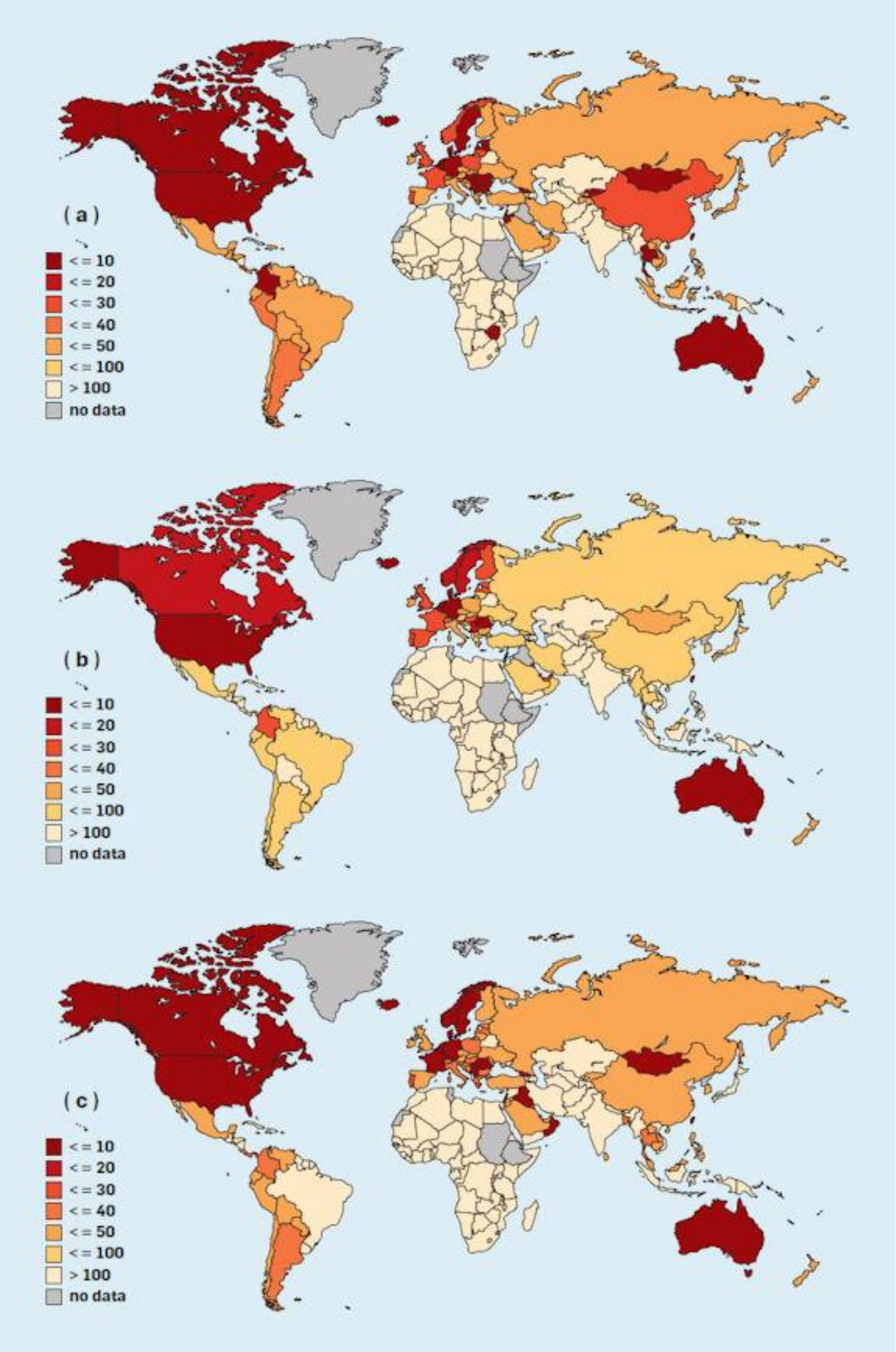
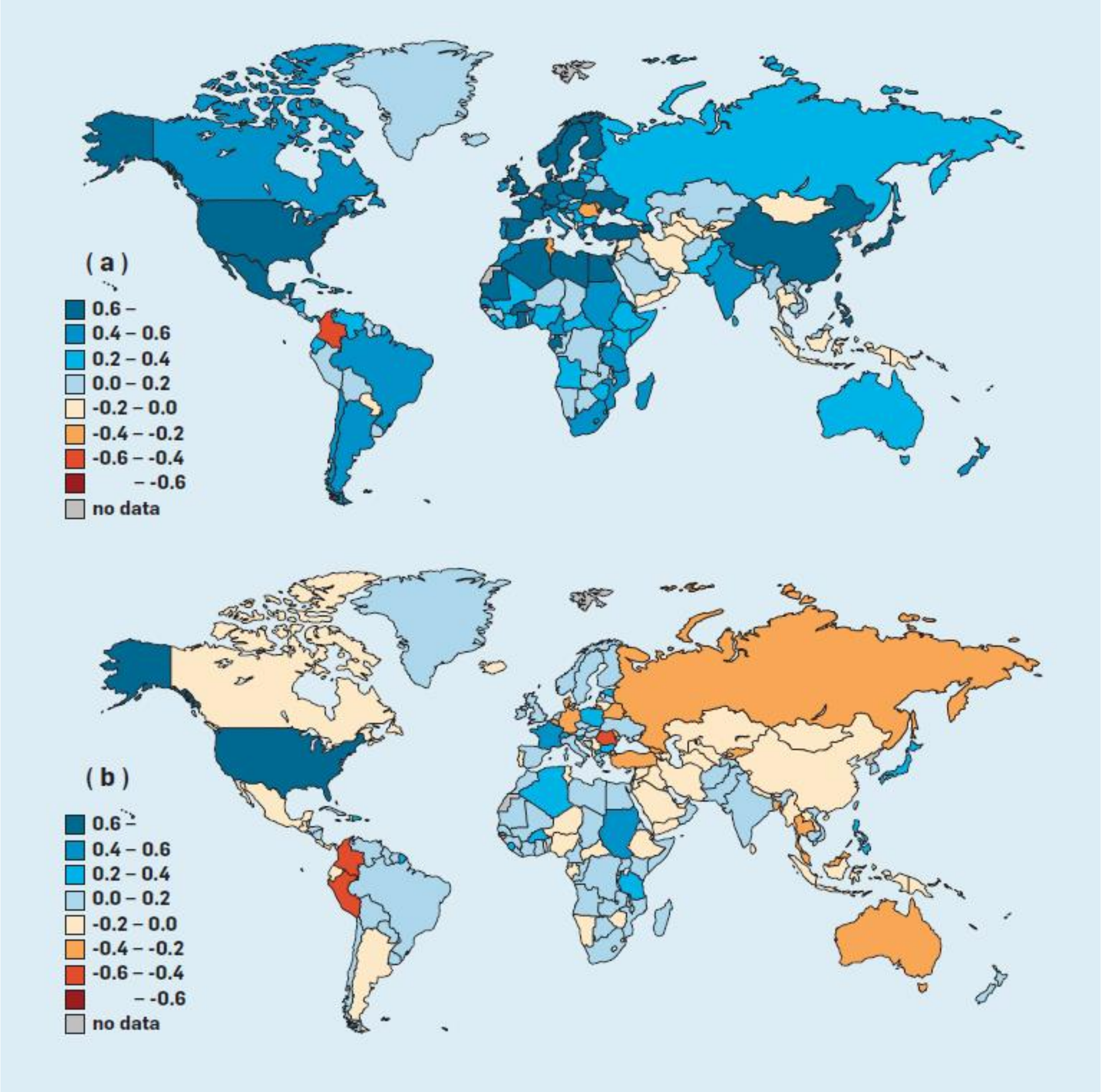
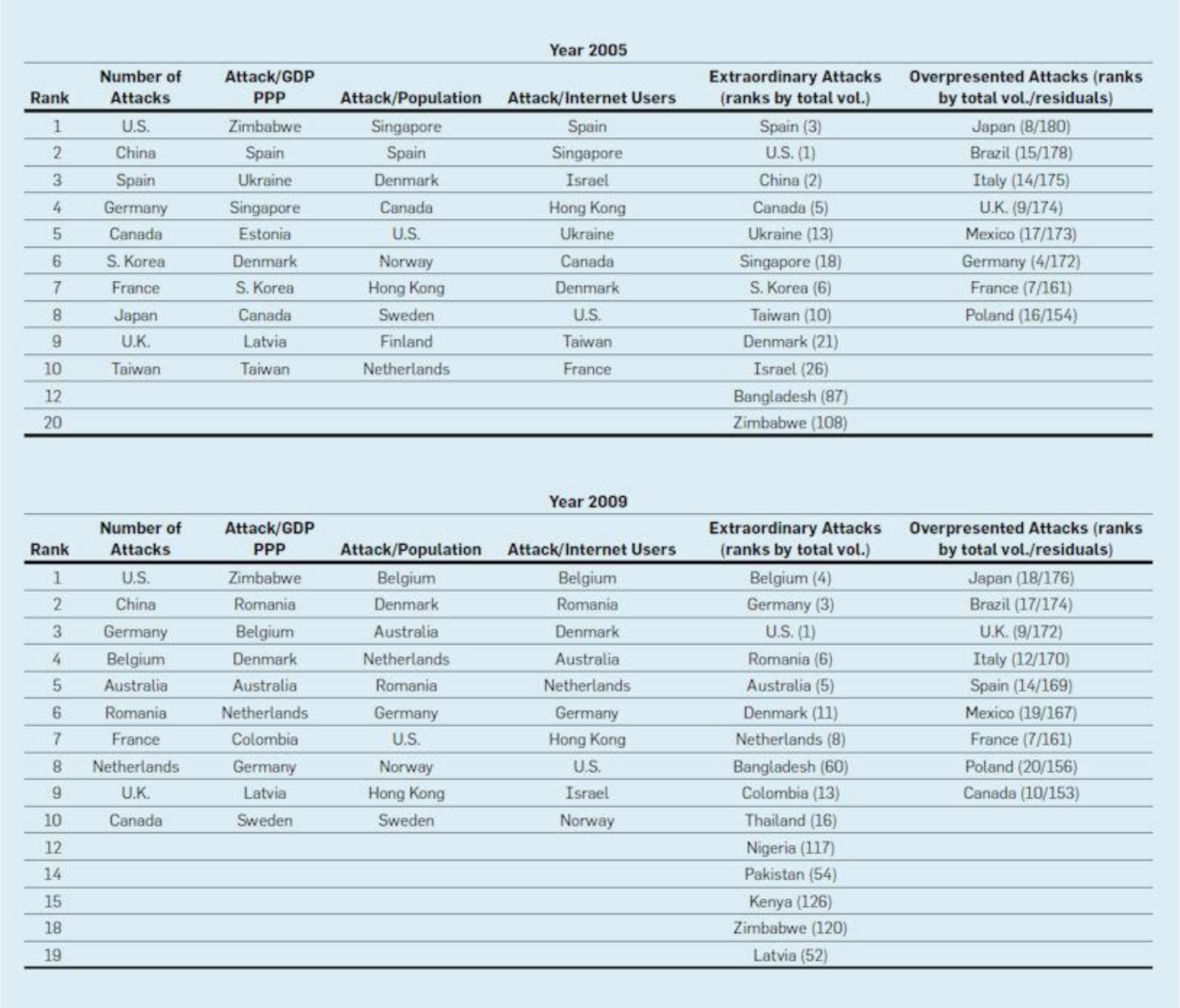


Figure 4. Correlation of (a) attack volume and (b) share of attack between the U.S. and other countries, 2005-2009.



Tables

Table 1. Top countries for originating attacks (by index).



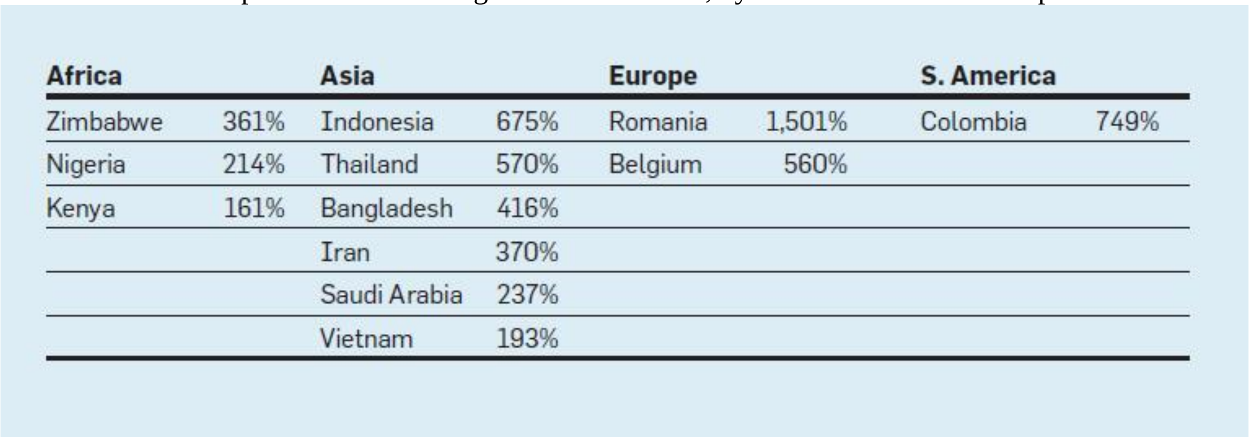
Year 2005

Rank	Number of Attacks	Attack/GDP PPP	Attack/Population	Attack/Internet Users	Extraordinary Attacks (ranks by total vol.)	Overpresented Attacks (ranks by total vol./residuals)
1	U.S.	Zimbabwe	Singapore	Spain	Spain (3)	Japan (8/180)
2	China	Spain	Spain	Singapore	U.S. (1)	Brazil (15/178)
3	Spain	Ukraine	Denmark	Israel	China (2)	Italy (14/175)
4	Germany	Singapore	Canada	Hong Kong	Canada (5)	U.K. (9/174)
5	Canada	Estonia	U.S.	Ukraine	Ukraine (13)	Mexico (17/173)
6	S. Korea	Denmark	Norway	Canada	Singapore (18)	Germany (4/172)
7	France	S. Korea	Hong Kong	Denmark	S. Korea (6)	France (7/161)
8	Japan	Canada	Sweden	U.S.	Taiwan (10)	Poland (16/154)
9	U.K.	Latvia	Finland	Taiwan	Denmark (21)	
10	Taiwan	Taiwan	Netherlands	France	Israel (26)	
12					Bangladesh (87)	
20					Zimbabwe (108)	

Year 2009

Rank	Number of Attacks	Attack/GDP PPP	Attack/Population	Attack/Internet Users	Extraordinary Attacks (ranks by total vol.)	Overpresented Attacks (ranks by total vol./residuals)
1	U.S.	Zimbabwe	Belgium	Belgium	Belgium (4)	Japan (18/176)
2	China	Romania	Denmark	Romania	Germany (3)	Brazil (17/174)
3	Germany	Belgium	Australia	Denmark	U.S. (1)	U.K. (9/172)
4	Belgium	Denmark	Netherlands	Australia	Romania (6)	Italy (12/170)
5	Australia	Australia	Romania	Netherlands	Australia (5)	Spain (14/169)
6	Romania	Netherlands	Germany	Germany	Denmark (11)	Mexico (19/167)
7	France	Colombia	U.S.	Hong Kong	Netherlands (8)	France (7/161)
8	Netherlands	Germany	Norway	U.S.	Bangladesh (60)	Poland (20/156)
9	U.K.	Latvia	Hong Kong	Israel	Colombia (13)	Canada (10/153)
10	Canada	Sweden	Sweden	Norway	Thailand (16)	
12					Nigeria (117)	
14					Pakistan (54)	
15					Kenya (126)	
18					Zimbabwe (120)	
19					Latvia (52)	

Table 2. Top countries with surged share of attacks, by % increase in 2009 compared to 2005.



Africa		Asia		Europe		S. America	
Zimbabwe	361%	Indonesia	675%	Romania	1,501%	Colombia	749%
Nigeria	214%	Thailand	570%	Belgium	560%		
Kenya	161%	Bangladesh	416%				
		Iran	370%				
		Saudi Arabia	237%				
		Vietnam	193%				