International Journal of Cybersecurity Intelligence & Cybercrime

Volume 1 | Issue 1 Article 2

8-2018

The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity

cybercrime, cyberterrorism, cybersecurity, IJCIC

Recommended Citation

Choi, Kyung-shick and Lee, Claire Seungeun (2018) The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity, International Journal of Cybersecurity Intelligence & Cybercrime: 1(1), 1-4. https://www.doi.org/10.52306/01010218YXGW4012

K. Choi., & C. S. Lee. (2018). *International Journal of Cybersecurity Intelligence and Cybercrime, 1* (1), 1-4.

The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity

Kyung-shick Choi, Boston University and Bridgewater State University, U.S.A

Claire Seungeun Lee*, Inha University, South Korea

Key Words: cybercrime, cyberterrorism, cybersecurity, IJCIC

Abstract:
Cybercriminology combines knowledge from criminology, psychology, sociology, computer science, and cybersecurity to provide an in-depth understanding of cybercrime. Cybercrime and cybersecurity are interconnected across many places, platforms, and actors. Cybercrime issues are continuously and expeditiously changing and developing, especially with the advent of new technologies. The International Journal of Cybersecurity Intelligence and Cybercrime (IJCIC) aims to contribute to the growing field of cybercriminology and cybersecurity. The IJCIC is eager to work with scholars, policy analysts, practitioners, and others to enhance theory, methods, and practice within cybercrime and cybersecurity at the regional, national, and international levels.

Cybercriminology is an interdisciplinary study that involves identifying the causes of cybercrime—combining knowledge from criminology, psychology, sociology, computer science, and cybersecurity—to deliver an in-depth understanding of the nature of cybercrime within the criminal justice system. Specifically, cybercriminology explores the causes and consequences of crime and deviance in cyberspace as well as its legal issues, ethics, prevention and control strategies. This is a field that is heavily invested in providing answers to law-making, law-breaking, and law enforcement processes, especially the process of making and enforcing laws that follow research in areas of criminal justice policy or law enforcement practices.

There are two research strands in cybercriminology. One is the application of general crime-related theories—for example, social control, self-control, lifestyle, delinquency theories—to cybercrime; whereas the other involves theory-testing or creating new theories to cybercrime. Cyber-routine activities theory (Choi, 2008; 2015) and space transition theory (Jaishankar, 2008) are such examples. However, what is still missing is perhaps more interdisciplinary perspectives and theories. In particular, linking social sciences (e.g. criminology, psychology, sociology and etc.) with technical perspectives (e.g. computer science, cybersecurity and etc.) is particularly important and highly needed. The Inter-

*Corresponding author
Claire Seungeun Lee, Ph.D., Assistant Professor of Sociology, Department of Chinese Studies, College of Humanities, Inha-ro 100, Inha University, Nam-gu, Incheon, South Korea, 22212
Email: clairelee@inha.ac.kr, drclaireselee@gmail.com

---

national Journal of Cybersecurity Intelligence and Cybercrime (IJCIC) aims to provide an avenue for this effort and make contributions to the growing field of cybercriminology and cybersecurity.

In an attempt to contribute to this emerging field, the International Journal of Cybersecurity Intelligence and Cybercrime aims to highlight the origins, patterns, causes, motivations, and trends of cybersecurity and cybercrime in a contemporary era, while also providing new methods and approaches to existing issues within the field. In this inaugural issue, we have six contributions including research articles, policy papers, and commentaries. These contributions provide international, global, and policy perspectives on illegal contents on social media, cyberterrorism, social engineering, hackers, and cyber social deviance. In addition, this inaugural collection of work advocates for a higher education cybersecurity interdisciplinary program to further the growth and knowledge within this field of study.

The proliferation of social media applications has increased the volume of harmful interactions and content online. Majid Yar (2018)'s paper entitled "A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media" adequately addresses this issue. In particular, sexually-oriented content regarding children and the racially or religiously hateful online content within the UK context. The changing nature of providers' unwillingness and/or inability to effectively stem the flow of illegal and harmful content has created a crisis for the existing self-regulatory model; consequently, we now move toward a much more coercive and punitive stance toward media platforms, so as to compel them into taking more concerted action.

Online hate speech—one of the cybercrimes discussed by Yar—was empirically tested in our next paper. With developed and intense technologies and Internet platforms, terrorists are able to manipulate the changing nature of cyberspace to their favor. Cyberattacks by both domestic criminals and foreign terrorists pose serious threats that require the FBI's attention (FBI, n.d.). Terrorists in cyberspace are increasingly utilizing social media to promote their ideologies, recruit new members, and justify terrorist attacks and actions. Kyung-Shick Choi, Claire S. Lee and Robert Cadigan (2018)'s paper entitled "Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS" adequately deals with the issue. Using a "global cyberterrorism dataset" with annual terrorist reports, court cases, and news reports from 2011 to 2016, Choi and his colleagues argue that different terrorist organizations use cyberspace and technologies differently. Al Qaeda-affiliated cyberterrorists, for example, use YouTube videos as both individual sources and embedded sources for Facebook and Twitter, whereas ISIS-affiliated cyberterrorists predominantly use YouTube videos and Twitter posts. This calls our attention to the different ways terrorists implement their recruitment and propaganda online as well as online hate speech.

In accordance with information technological development, hacking has become a pervasive form of crime worldwide in recent years. In this regard, "Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory" by Sinchul Back, Sadhika Soor, and Jennifer LaPrade used an existing survey on middle school and high school students in the United States, Russia, Spain, Venezuela, France, Hungary, Germany, and Poland comparatively (Back et al., 2018). Their results show strong support of Michael Gottfredson and Travis Hirschi's (1990) self-control theory and partial support for Hirschi's (1969) social bond theory.

A policy paper by Katalin Parti, Tibor Kiss, and Gergely Koplányi— "Architecture of aggression in cyberspace: Testing cyber social deviance in youth utilizing the Bryant-Smith Aggression Scales"—tested the online aggression-violence scale on a sample of young adults (aged 19-24) studying in law schools and social work bachelor of arts courses throughout Hungary. Parti and her colleagues

found that cyberspace, online anonymity, and online social networking sites, do not work as a catalyst of social violence. Their study emphasizes that while higher education has a significant role in establishing control, better teaching nonviolent communication, and coping strategies should be further developed. One way is to offer coordinated school-based anti-bullying programs across different disciplines (Parti et al., 2018).

Finally, Dennis Giever presents a compelling argument for interdisciplinary programs in cybersecurity at the university level in his commentary—"An Argument for Interdisciplinary Programs in Cybersecurity" (Giever, 2018). We now live in a society where IT security and physical security do not have boundaries. He recommends that any security program take on a "all possible paths" or "balanced approach" to the protection of assets within an organization. Students in computer science, criminal justice, business, and human resources (among others), should learn and work collaboratively with other disciplines. A collaborative effort is also important to accomplish the myriad of tasks necessary to protect assets today.

Cybercrime and cybersecurity are ubiquitous and interconnected across different platforms, places, and actors. These issues are rapidly changing and developing with new skills and technologies. We look forward to receiving contributions from scholars, policy analysts, practitioners, and others on enhancing theory, method, and practice within the field of cybersecurity and cybercrime on national, regional, and international dimensions.

References

Back, S., Soor, S., & Jennifer LaPrade (2018). Juvenile hackers: An empirical test of self-control theory and social bonding theory. *International Journal of Cybersecurity Intelligence and Cybercrime, 1*(1), 40-56.

Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*, 308–333.

Choi, K.-S. (2015). *Cybercriminology and Digital Investigation.* LFB Scholarly Publishing LLC.

Choi, K.-S., Lee, C. S. & Cadigan, R. (2018). Spreading propaganda in cyberspace: Comparing cyber-resource usage of al qaeda and ISIS", *International Journal of Cybersecurity Intelligence and Cybercrime, 1*(1): 21-39.

FBI. (n.d.). Cyber Crime. Retrivied from https://www.fbi.gov/investigate/cyber.

Giever, D. (2018). "An argument for interdisciplinary programs in cybersecurity. *International Journal of Cybersecurity Intelligence and Cybercrime, 1*(1), 71-76.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime.* Stanford University Press.

Hirschi, T. (1969). *Causes of delinquency.* Berkeley: University of California Press.

Jaishankar, K. (2008). *Space Transition Theory of cyber crimes.* In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

Parti, E., Kiss, T., & Koplányi, G. (2018). Architecture of aggression in cyberspace: Testing cyber social deviance in youth utilizing the Bryant-Smith Aggression Scales. *International Journal of Cybersecurity Intelligence and Cybercrime, 1*(1), 57-70.

Yar, M. (2018). A failure to regulate? The demands and dilemmas of tackling illegal content and behaviour on social media. *International Journal of Cybersecurity Intelligence and Cybercrime, 1*(1), 5-20.

Wetten, J. (2005, November). Time to get physical. *Redmond Magazine*, 67-68.