



Fall 2012

Batter Up: Who's Prepared to Take the Hit from the Stuxnet Aftermath?

Kortney Mosley

Follow this and additional works at: <https://engagedscholarship.csuohio.edu/inthebalance>

 Part of the [Computer Law Commons](#), and the [International Law Commons](#)

[How does access to this work benefit you? Let us know!](#)

Recommended Citation

Mosley, Kortney, "Batter Up: Who's Prepared to Take the Hit from the Stuxnet Aftermath?" (2012). *In the Balance*. 24.

<https://engagedscholarship.csuohio.edu/inthebalance/24>

This Monthly Feature is brought to you for free and open access by the Journals at EngagedScholarship@CSU. It has been accepted for inclusion in In the Balance by an authorized administrator of EngagedScholarship@CSU. For more information, please contact library.es@csuohio.edu.

Batter Up: Who's Prepared to Take the Hit from the Stuxnet Aftermath?

December 6, 2012

By: Kortney Mosley, Associate, The Global Business Law Review

Economists have described cyberspace as the “fifth domain of warfare”^[1]. Vast advancement in technological resources has led to a surge in cyber attacks that are more prevalent in our society than traditional modes of warfare. Cyber war can be defined as, “action by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.”^[2]

In light of the ongoing conflict between Israel and Iran, Israel along with the United States initiated a set of cyber attacks toward Iran, the most common being the “Stuxnet”^[3]. Stuxnet was accidentally discovered during the summer of 2010 when the virus emerged as the result of a programming error that escaped the facility of the intended target, Iran’s Natanz Plant and was viewed worldwide.^[4] The purpose of Stuxnet was to disrupt Iranian nuclear plants’ operation of the gas centrifuges used to make highly enriched uranium, the critical component in the creation of nuclear weapons.^[5] This attack was triggered by President Obama’s acceleration of “Code Olympic Games,” initially developed under the Bush Administration.^[6] Stuxnet was initially introduced using a USB port, a source independent to Internet connection.^[7] Specifically, Stuxnet strikes by exploiting vulnerabilities in the Windows operating system, which allows the injection of malicious codes into the nuclear plant computer systems.^[8]

Stuxnet had a large impact on Iranian nuclear plants. A few weeks after Stuxnet was detected, almost one-fifth of the centrifuges spinning to purify the uranium were affected.^[9] Iran believes the Stuxnet virus, initiated the first stages of cyber war—one which sets the stage for Iran to create their own cyber command in response to future viruses.^[10] Experts say that the United States remains “woefully unprepared” to defend itself if Iran were to launch a similar attack.^[11] The United States’ involvement poses a significant question, “are we prepared to take the hit?”

^[1] See *War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict*, The Economist (June 1, 2010), <http://www.economist.com/node/16478792> (discussing how cyber space is the fifth domain of warfare after land, sea, air, and space).

[2] Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 Cal. L. Rev. 817, 823 (2012).

[3] *Cyberattacks on Iran-Stuxnet & Flame*, N.Y. Times (Aug. 9, 2012), http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html?8qa [hereinafter *Cyberattacks on Iran-Stuxnet & Flame*].

[4] *Id.*

[5] John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 J. Marshall J. Computer & Info. L. 1, 4 (2011).

[6] *Cyberattacks on Iran-Stuxnet & Flame*, *supra* note 3.

[7] William M. Stahl, Note, *The Uncharted Waters of Cyberspace: Applying the Principles of Maritime Law to the Problem of Cyber Security*, 40 GA. J. Int'l & Comp. L. 247, 260 (2011).

[8] *Id.*

[9] *Cyberattacks on Iran-Stuxnet & Flame*, *supra* note 3.

[10] Cassandra M. Kirsch, *Science Fiction No More: Cyber Warfare and the United States*, 40 Denv. J. Int'l L. & Pol'y 620, 642 (2012).

[11] Gary Smith, *Stuxnet: US Can Launch Cyberattack But Not Defend Against Them, Experts Say*, Huffington Post (June 10, 2012), http://www.huffingtonpost.com/2012/06/01/stuxnet-us-cyberattack_n_1562983.html.