ISSUE BRIEF

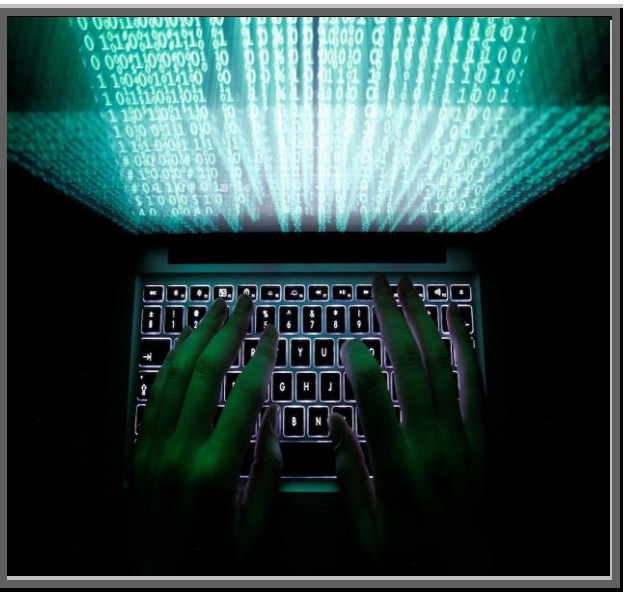
INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

ESCALATING CYBERWARFARE IN THE MIDDLE EAST

By
Aamna Rafiq
Research Associate
Arms Control & Disarmament Centre, ISSI

Edited by
Najam Rafique

October 25, 2020



As Iran marked the 10th anniversary of the Stuxnet,[1] its nuclear facilities were again hit by a large number of cyber attacks which Behrouz Kamalvandi, Spokesperson of the Atomic Energy Organization of Iran (AEOI) also confirmed.[2] However, these attacks did not cause any substantial damage as Iran blocked them on time. With increasing technological development and digitalization in the last decade, the number of cyberattacks against critical infrastructure has increased in the Middle East. The escalating cyberwarfare will breed further instability in the crisis ridden region.

What makes cyberwarfare in the Middle East more dangerous and distinct from the rest of the world is the sophistication and exclusivity of cyberattacks. Stuxnet was designed to infect the computer systems connected to the specific "programmable logic controllers (PLCs)" at Iran`s Natanz uranium enrichment facility. Stuxnet targeted specific models of PLCs which were exclusively manufactured by Siemens. In addition to 30,000 computers, 1000 centrifuges at the Natanz uranium enrichment facility were damaged.[3] The core objective was to deter Iran from achieving the nuclear weapon capability by inflicting irreversible damage to Iranian nuclear program via cyber-weapon. Wiper was

1 Stuxnet is a highly complex, malicious and customized computer worm, first discovered in June 2010. It is known as the world`s first-ever cyber weapon.

2 "Iran halts numerous cyber-attacks on nuclear plants," *Middle East Monitor*, accessed on September 28, 2020, https://www.middleeastmonitor.com/20200907-iran-halts-numerous-cyber-attacks-on-nuclear-plants/.

3 Andrew Hanna, "The Invisible U.S.-Iran Cyber War," *The Iran Primer*, July 23, 2020, https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war.

another dangerous malware that hit the computer systems of the National Iranian Oil Company and Iranian Oil Ministry in April 2012. Wiper was designed to completely and systematically destroy the data stored in the hard drive of the infected computer system. Afterwards, Wiper also erased system files causing the entire computer system to crash without leaving any mark of infection behind.[4] Wiper is a sophisticated and unique cyber weapon which led to three fascinating developments in the Middle East.

First, Wiper led to the development of another malware popularly known as Shamoon. Technically, Shamoon was a cheap and less sophisticated version of Wiper and mainly targeted the critical computer systems of Aramco - the biggest Saudi oil giant. Secondly, Wiper gives preference to the files stored in ".pnf extension" during the erasing process. What makes this entire saga more interesting is the fact that this extension was not only an uncommon format but also used by the Stuxnet to store its files.[5] Therefore, Wiper was designed either as an antidote to Stuxnet or to trace the computer systems infected with Stuxnet. This raises serious questions regarding the motive and actors behind Wiper. Lastly, the discovery of Wiper led to the discovery of Flame worm in Middle Eastern countries, especially Iran. Flame is a giant espionage worm which installs itself in pieces without raising any red flags.[6] According to various official and unofficial sources, all three cyber weapons – Flame, Wiper, and Shamoon have made a huge comeback in the last two years. According to Kaspersky, Flame shares a lot of features with Stuxnet but it is twenty times more complicated than Stuxnet.[7]

As the cyberwarfare is gaining momentum in the Middle East, it has also set the concept of "cross domain deterrence" (CDD) in motion. CDD refers to employing capabilities in one domain of military operations to deter adversary`s potential act of aggression in another domain. The United States (US) introduced CDD to achieve its strategic objectives in the post-cold war global strategic landscape comprised of asymmetric, complex and hybrid threats in traditional (land, air, sea) as well as new (outerspace, cyberspace) domains.[8] CDD would seriously affect the regional peace as it gives an opportunity to one of the key players in the Middle East to initiate a conflict by conducting a military operation in one of the five domains. The aggressor will continue to vertically escalate the violence till it reaches the threshold in that particular domain. At this stage, the aggressor can

4 Kim Zetter, "Wiper Malware That Hit Iran Left Possible Clues of Its Origins," *Wired*, accessed October 5, 2020, https://www.wired.com/2012/08/wiper-possible-origins/.

5 Ibid.

6 Kim Zetter, "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers," *Wired*, accessed October 5, 2020, https://www.wired.com/2012/05/flame/.

7 Ibid.

8 King Mallory, "New Challenges in Cross Domain Deterrence, Perspective," RAND Corporation (2018), https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE259/RAND_PE259.pdf.

escalate horizontally by shifting the conflict to a second domain. In this way, the aggressor will not only gain the escalation dominance but also vertically escalate an overall conflict without all-out war in any single domain.[9] This strategy was used in June 2019 when US carried out a cyberattack, instead of an air strike, in retaliation to the Iranian attack on the US surveillance drone in the Strait of Hormuz. This cyberattack by the US Cyber Command incapacitated multiple computer systems controlling the Iranian missile launch system[10] without giving Iran the raison d'être for a retaliatory strike.

The sophistication and complexity of cyber weapons used in the Middle East requires huge financial and human resource investment in gathering accurate technical information about the targeted systems. This intelligence gathering is practically impossible without an insider support. Furthermore, developing a complicated cyber weapon requires a high level of research and development which is technically impossible for a non-state actor to possess. Flame and Wiper were reportedly developed around 2005. In 2013, the Symantec Corps reported that the Iranian nuclear facilities were targeted with an early version of Stuxnet in 2007. The similar timeline, close technical linkages among cyberweapons and geographical proximity of the targets indicates that Flame and Wiper were designed either by the states that designed Stuxnet or states that probably got access to the original Stuxnet files.

Targeting the counter-value targets is another recent trend in the Middle East to look for. The financial sector, sea ports, oil, and gas industry are top targets of cyber warfare. In 2019, more than half of cyberattacks in the Middle East were directed against the oil and gas industry.[11] The significance of Middle Eastern states in the global strategic landscape primarily depends on their role in global oil and gas market. Therefore, every cyberattack on the oil industry is a calculated strategic move with far-reaching impact on regional economy and global energy balance. The selection of counter-force targets like nuclear facilities and missile control systems clearly indicate the illicit motive of inflicting huge damage to the national defence of a targeted state. This makes the Middle East a classic case of cyber realism where cyberspace is just another domain where states have brought their pre-existing conflicts, territorial disputes, power struggles, blame casting, strategic interests, and security dilemma. The operationalization of CDD will breed more chaos in each domain. Calculating a threshold level for each player in five domains at a particular moment on an

9 Ibid.

10 Julian E. Barnes and Thomas Gibbons-Neff, "US Carried out Cyberattacks on Iran," *The New York Times*, last updated June 22, 2019, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.

11 Weizhen Tan, "Cyberattacks in the Middle East are on the rise. Here's who they're targeting," *CNBC*, accessed on October 5, 2020, https://www.cnbc.com/2019/06/18/cyberattacks-in-uae-middle-east-darkmatter-report.html

escalation ladder is extremely risky. Any lapse in escalation control or misunderstanding in strategic signalling could result in an all-out war.