International Studies Perspectives (2015) **0**, 1–15

Israel and Cyberspace: Unique Threat and Response

Matthew S. Cohen
Northeastern University

Charles D. Freilich
Harvard University
AND
Gabi Siboni
Institute for National Security Studies

This article provides insights into the dangers and opportunities that the cyber realm poses to states by conducting the first comprehensive case study on Israeli use of cyberspace. Israel faces a constant barrage of cyberattacks from actors ranging from states to hacker groups to individuals. This has forced Israel to develop highly advanced capabilities. Israel has not just faced cyberattacks but has also been a leader in using the cyber realm for offense. Although the threats to Israel are severe, they are not unique; thus, Israel can serve as a model for what other states can do to effectively use cyberspace both defensively and offensively. This article offers policy recommendations as to how states can improve their cyber defenses.

Keywords: cybersecurity, cyber war, Israel, cyberspace

Israel, a state that relies heavily on cybertechnology, is particularly vulnerable to cyberattacks and has been a primary target thereof (Ben-David 2011, 57; Clarke and Knake 2012, 155). Indeed, Israel faces a nearly constant barrage of cyberattacks, roughly 1,000 every minute in 2012 (Eisenstadt and Pollock 2012; Grauman 2012, 66). During the 2014 operation against Hamas in Gaza, Israel faced over 1 million cyberattacks every day (Shamah 2014).

Although there is an ongoing academic debate (e.g., Demchak 2011; Nye 2011; Clarke and Knake 2012) regarding the actual severity of the cyber threat, and different countries have responded to it in various ways, Israel has taken it very seriously, defining the cyber threat as one of the gravest threats it faces and rapidly developing capabilities that have placed it at the forefront of the cyber world. Israel has been a leader in using the cyber realm for offense as well. Indeed, Israeli policies on cyber defense are trend setting and have been cited as an example of what the rest of the world should attempt to emulate (Grauman 2012). Major technology companies have taken notice of Israel's accomplishments and have established offices in Israel, and Israel additionally boasts a large number of start-up companies in the cyber realm (Eisenstadt and Pollock 2012, xiii, 32; Steinherz 2014).

Studies of national cyber policies have been conducted on only a handful of states, and there is no truly comprehensive academic study of Israeli policy and

Cohen, Matthew S., Charles (Chuck) D. Freilich and Gabi Siboni. (2015) Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives*, doi: 10.1093/isp/ekv023