# **Stuxnet: The World's First Cyber... Boomerang?**

Stuxnet – "the world's first fully fledged cyber weapon" was engineered by the United States and Israel as part of a wider covert operation aimed at undermining the Iranian nuclear program. Whilst the United States and Israel had long been suspected of developing this complex piece of malware, Sanger described the nature of their involvement more fully than any previous account.

This release of the worm is likely to have: fueled an on-going cyber arms race by demonstrating to other nations the strategic utility of cyber weapons; elevated the severity of the cyber threat by providing a broad range of actors with a template from which to construct their own cyber weapons; set a precedent for the use of cyber weapons as instruments of state policy.

Stuxnet, however, is widely regarded as a "game changer". Unlike the malware used in previous cyberattacks, it was highly targeted and designed to achieve a real world outcome.1 As Industrial Control System (ICS) security analyst Ralph Langner notes, rather than being designed for denial of service attacks or industrial espionage, "Stuxnet's goal was to physically destroy a military target not just metaphorically, but literally".

It is quite clear that the goal of Stuxnet was to disrupt Iran's nuclear enrichment program. This highly sophisticated weaponized worm may have achieved its objective, but this is likely to have come at a cost; a cost which may in fact someday come back to harm its original creators.

- C.Meghana Reddy

CSE-III C

179X1A05E0