# Weaponizing the internet for terrorism

May 16 2017

Credit: George Hodan/Public Domain

Terrorism is a fact of life as are the collectives and networks to which counter-terrorism organizations and the media have given various labels and names. These networks are well versed in exploiting modern information technology through social media awareness, marketing and recruitment campaigns. However, there is the more insidious use by terrorists groups of online networks and exploits in the creation of so-called bots (computers that have been compromised through the implementation of malware and control over which has been assumed by a third party, or more likely a third party control a lot array of such bots in a botnet.

Writing in the *International Journal of Collaborative Intelligence*, Emmanuel Ogu of the Department of Computer Science, at Babcock University, in Ilishan-Remo, Ogun State, Nigeria, and colleagues suggest that the problems caused by botnets in terms of interfering with infrastructure, healthcare services, transport, power supply and other critical parts of the modern world are not very different to those caused by the more familiar notion of terrorist attacks involving explosives and weapons. Events across the globe in mid-May 2017 saw the rapid and devastating spread of ransomware to hospitals, companies, organizations, and individuals. Whether or not this was a specific attack by a particular group is irrelevant the impact was enormous on those waiting for healthcare attention, for instance.

A similar "attack" on an even bigger scale might see power supply outages brought about by malware-toting botnets operated by those with malicious intent where there is no simple financial extortion, rather crippling and even destruction of infrastructure is the aim of the perpetrators.

"Fighting bots and keeping them away from network infrastructures has gradually become the nightmare of every network security professional," the team says. Fundamentally, this is because although individual computers may be wiped of malware and systems patches or a botnet disabled, the distributed and infectious nature of the computer viruses, worms and other malware that propagate the controls with which the "botmaster" will rally the compromised computers are always being modified to counteract antivirus software. The researchers warn that research shows we are not too far away from a new wave of insurgency and terrorism that may gradually overtake the internet and many organizational network infrastructures around the world.

"Just as the secret to dismantling terrorist networks have been proven to lie in destroying the ability of the terror group to recruit, train, control and coordinate their activities (essentially by completely taking out their command and control infrastructure), the secret to ridding the internet of botnets, perhaps, also depends on similar means," the team suggests. "Intelligence reports are useless if they do not lead to informed decisions and actions," they add. Warnings of out of date operating systems, web browsers and email programs, unpatched computers, and the non-implementation of firewalls and antivirus software seem to be unheeded in too many cases. If those warnings are left unheeded by the users of infrastructure critical computers in healthcare, transportation, industry, power supply other areas, then the inherent vulnerabilities might be exploited by those with malicious intent repeatedly whether for financial gain, terrorist propaganda and control or both.

**More information:** Emmanuel C. Ogu et al, Insights from terrorism intelligence and eradication efforts - Al-Qaeda, ISIS, Boko Haram - for more pragmatic botnet countermeasures, *International Journal of Collaborative Intelligence* (2016). DOI: 10.1504/IJCI.2016.084115

Provided by Inderscience Publishers

Citation: Weaponizing the internet for terrorism (2017, May 16) retrieved 7 May 2024 from https://techxplore.com/news/2017-05-weaponizing-internet-terrorism.html