FUTURE
for Advanced Research & Studies

Artical Name : The “Militarization” of the Internet in the Syrian Conflict

Artical Subject : The “Militarization” of the Internet in the Syrian Conflict

Publish Date: 09/11/2016

Auther Name: Future for Advanced Research and Studies

Subject :

The usage of the internet for military purposes has substantially evolved within recent decades, in light of the notable success in the conquest of space and the advancement of satellite technology. The intersection of outer space and cyberspace has been molded to serve military purposes, to set up firewalls against potential threats. Various recent studies on the topic of the militarization of the internet have stated that developments in this field have come as a reaction to perceived threats, in addition to the aim of enhancing military capabilities. In other words, it could be said that the growing use of the “military internet” is taking place in the midst of a “technology race” between major world powers, whose interests and policies diverge with regards to numerous regional and international issues. The conflicts and crises which the Middle East is currently experiencing, especially since the uprisings of 2011, have doubtlessly contributed to the region becoming a testing field for internet militarization. This is most clear in the Syrian conflict, which has proved extremely polarizing in the international arena. An Open ArenaThe Syrian conflict has entered a new phase with the escalation of Russian political and military intervention in support of the Assad regime against the armed opposition and Jihadist groups. The Russians have recently disclosed their usage of the latest internet-dependent military technologies, as Russian military units have deployed the latest generation of high-speed communications and cyber-warfare systems, epitomized by the “R-169” and “B-380 K” systems. Moscow has also tested new systems for signal jamming and electronic warfare, seeking to obtain specific information from closed audio communications which are shielded by advanced protection systems, as well as protecting the communications of Russian forces from being hacked by hostile entities. Securing communications between the different branches of Russian forces in Syria is not Russia’s only objective. It has established a secure network, which it calls the “Close Data Transfer Network”, in response to measures taken by other actors, such as Turkey, which has established a special electronic signal jamming system - ‘KORAL’ -on the Turkish-Syrian borders, designed to compromise the effectiveness of the Russian air defense system “S 400”, tasked with the defense of the Syria-based Russian air base in Hameimim.Russia has not stopped there. According to several reports, it has transferred its latest surveillance craft, TU-214R, to Hameimim base at the end of February 2016. The drone is equipped with ray emitting reconnaissance equipment and signal-jamming devices, which are capable of intercepting radio signals from mobile phones, as well as signals from planes and ground radars and electronic warfare systems. The intention behind this action is to track the movements of militant organizations, especially during times of ceasefire. Doubtlessly, the shooting down of the Russian fighter jet Sukhoi Su-24 in November 2015, has also contributed to the Russian decision to transfer the new systems into Syria. There may also be a promotional aspect to the decision, given Russia’s wish to test and show off its new weapons systems in Syria.It cannot be said that Russia is unique in its deployment of these types of technology in Syria, as Iran has also played a similar role. Iran assisted the Assad regime with internet surveillance technology designed to counter popular demonstrations, a method which the Iranian paramilitary Revolutionary Guard applied in 2009 in its crackdown on the protests following the presidential elections of that year, commonly known as the “Green Revolution”. The Revolutionary Guard was able to track the actions of youths on social media, SMS, and e-mail.While Iran initially provided surveillance equipment and drones to help the Assad regime monitor anti-regime protesters, especially on social media, it soon escalated its assistance by providing finances and forming and training sectarian militias made up of several nationalities: Iraqis, Lebanese, Iranians, Pakistanis and Afghanis, which provided armed support to the Syrian government. Potential DangersThere are rising concerns that the various actors providing the Syrian regime with technological, economic and military assistance, ultimately seek to spy on the entirety of internet usage in Syria. The surveillance would encompass both the Syrian opposition and militant groups, as well as the various components of Syrian society. This warning is based on a number of indicators related to the slowness and frequent disconnections plaguing internet services in Syria. Neither the regime nor the opposition have provided official explanations of this phenomenon . The opposition have suspended internet services in some areas on more than one occasion,, most recently in October of 2016, citing hacking-related security concerns necessitating cutting off the internet in Aleppo, and threatening penalties against those who violated their dictates. These concerns were strengthened by the presence of a Russian spy ship in early October 2016 in the vicinity of sea cables extending between Turkey and Cyprus, indicating that its target may have been spying on Syrian cyberspace. These suspicious have been expressed repeatedly by social media activists, and by a cyber-security website that called on internet users in Syria to exert extreme caution, particularly when using services easily intercepted such as Skype.What is most striking in this context is that the evidence points to the possibility that Russian aims extend beyond Syria, into countries neighboring it, especially Turkey. Russian-Turkish tensions escalated sharply after the downing of the Russian jet in November 2015, before gradually calming following an official apology for the incident from Turkish president Erdogan in June 2016. In view of all this, it may be said that the utilization of what has been dubbed “military internet” is expected to increase in the coming period, in view of Russia’s insistence on escalating its intervention in the Syrian conflict, its fears of cyber-attacks against its armed forces, and Iran’s continued financial, military and technological support for the Syrian regime. In all events, Syria has become a testing field for the technological military capabilities of the different powers embroiled in its civil war.