Fall August 8, 2014

African nations as proxies in covert cyber operations

Jan Kallberg, *University of Texas at Dallas*
Steven Rowlen, *Arkansas Tech University*

African nations as proxies in nation states' covert cyber operations

Jan Kallberg and Steven Rowlen

PUBLISHED IN "AFRICAN SECURITY REVIEW" – THIS IS THE ACCEPTED MANUSCRIPT AND DIFFER FROM THE ACTUAL PUBLISHED. IF CITING, READ THE PUBLISHED VERSION AD CITE "AFRICAN SECURITY REVIEW".

Abstract

The growth of the African Internet, and services related to the Internet, has been rapid over the last decade. Following this market expansion, a variety of service providers have started to provide access. A fast--growing market put pressure on the providers to deliver services first and only then ~~afterward~~ seek to secure the networks. Over time, ~~have~~ the industrialis~~z~~ed nations have become more able to detect and trace cyber -~~attacks~~ against their networks. These tracking features are constantly developing and the precision in determining the origination of an attack is increasing. A state--sponsored cyber -~~attacker~~, such as intelligence agencies and electronic warfare units, will seek to avoid detection, especially when the attacks are politically sensitive intelligence gathering and intrusion into foreign states' networks. One way for the attacker to create a path that links the attacks and the originating country is by actions through a proxy. The less technologically mature developing nations offer an opportunity for cyber aggression due to the lower level of security under the quick expansion of the Internet-based market. Developing countries could be used as proxies, without their knowledge and consent, by the unauthoris~~z~~ed usage of these countries' information systems in ~~the pursuit of~~an attempt to~~an~~ attack ~~on~~ a third country by a state--sponsored offensive cyber operation. If the purpose of the cyber -~~attack~~s is to destabilis~~z~~e a targeted society and the attack succeeds, the used proxies are likely to face consequences in their relations with foreign countries, even if the proxy was unaware of the covert activity.

Introduction

The growth of the African Internet, and services related to the Internet, has been rapid over the last decade. Following this market expansion, a variety of service providers have started to provide access. A fast--growing market put pressure on the providers to deliver services first, and only then ~~afterward~~ seek to secure the networks. Parallel with this development, ~~have~~ foreign state actors have been driving an~~en to~~ increasingly militarised~~zation of the~~ Internet, where state actors seek an intelligence and political advantage, leading to ~~a~~ new territory for covert actions against other states.[1]

Until now, these covert cyber operations had~~ve~~ benefitted from the inability to technically attribute the attacks to a perpetrator due to lack of traceability. Until recently, i~~I~~t ~~had earlier been~~was unlikely that an attacker in cyberspace would risk being held accountable or exposed as the perpetrator. The early Internet had limited technical abilities to track from where a cyber-attack originated. Over time, ~~have~~ the industrialis~~z~~ed nations have become ~~more~~ better able to detect and trace cyber -attacks against their networks. These tracking features are constantly developing and their precision in determining the origination of an attack is increasing. A state--sponsored cyber -attacker, such as intelligence agencies and electronic warfare units, will seek to avoid detection, especially when the attacks are politically--sensitive intelligence gathering and intrusion forays into foreign states' networks. One way for the attacker to create a path that links ~~between~~ the attacks and the originating country is~~are~~ actions through a proxy. The less technologically mature developing nations offer an opportunity for cyber aggression due to ~~the~~ a lower level of security under the quick expansion of the Internet-based market.

Formatted: Font: Not Italic

The Aggressors' Advantage

Historically, since the Internet started to become a common feature in our lives, independent hackers have been seen as a major threat in the public discourse. Contrary

to common beliefs, the first ~~twenty~~ 20 years of the Internet was acceptably secure, due to the limited abilities of the attackers, compared to the threat generated from a militari~~s~~z~~z~~ed Internet with state actors conducting cyber operations. The early cyber ~~-~~attacks were simplistic and lacked any goals beyond short ~~-~~term financial gain through credit card theft and financial fraud.

Instead of moving towards increased security over time, the Internet has had a reverse~~d~~ trajectory where it has become ~~more~~ increasingly unsafe over time due to the ~~increasing~~growing presence of highly funded state actors. The entry of state actors created~~-~~ a contested cyberspace, where intelligence, economic espionage, information operations, and psychological operations radically changed the fundamentals for Internet security.

The aggressive state actor has an advantage in cyberspace due to the weaknesses in attribution, which works as a standing invite to conduct proxy wars, utili~~s~~z~~-~~ing criminal networks or aligned political groups~~,~~ to carry out the attacks with little risk ~~for~~ of detection from networks in third countries. ~~In plain English~~Simply put, if the Revolutionary Guard of Iran sought to attack ~~American~~ United States (US) or British networks, they would avoid direct responsibility by ~~only~~ creating the code and, under specific circumstances, running the attack from hijacked computers in, ~~as an~~for example, Botswana. Another alternative is, ~~to, under~~ in a short period of time, to fly ~~in~~ their operatives into a country in the developing world to carry out ~~actions~~ the attack using Internet access gained ~~from a~~under the false pretence of conducting business or any other lawful purpose.

This requires a modified view on the role of cyberspace ~~role~~ in national security for the developing world, as these nations are at a greater risk ~~for~~ of being proxies for cyber ~~-~~attacks targeting foreign countries. The level of awareness and susceptibility to

cyber -attacks is reflected by the maturity and development of a country's I~~i~~nternet infrastructure, ~~of a country~~ as emerging Internet communities lack the experience of complex attacks. Keren and Elazari find that Africa has the lowest Cyber Attack Susceptibility (CAS) score of all regions (quantified based on usage, online services rendered, telecom infrastructure, and human information technology capitol for each country) and the lowest variances.[2] A higher CAS score implies that the country is more susceptible to an attack that directly ~~attack~~ targets the I~~i~~nternet usage of users, as more connected users will be affected during any given attack, but it also reflects technological maturity and experience with hijacked computer networks and systematic intrusions. The low CAS score for Africa indicates that the region is likely to be emerging as an information-based society, and that the growth of the networks prevails over consolidation.

According to Fahrenkrug,[3] ~~,~~ the attacker has the advantage in cyberspace and the cost of defensive measures easily outpaces the cost to produce a cyber -weapon. The only deterrence that exists for cyber -attacks is attribution that can lead to political, diplomatic, and financial repercussions.

The scenario becomes more complex if a state actor gathers information about cyber vulnerabilities in the networks of a targeted organis~~z~~ation or other nation and then outsources the attack to a criminal or terrorist network. There will be no forensic link to trac~~k~~ if there are no operatives flying in or no systems accessed to attack a third country.

This innovative approach creates numerous obstacles and considerations for the targeted organis~~z~~ation. First, the attribution problem is highlighted because even if the executing criminal network is identified, it is still unclear which actor initiated the attack. Criminal networks are enterprises and the compensation could be a range of

illicit goods.[4] States can pay to get things done. If necessary, a covert operating state can pay criminal networks in cash, drugs, weapons, or any other currency to act as a proxy.

Second, the lack of attribution evaporates the option to initiate retribution against the initial attacker. Attribution can be very hard to achieve if the host or proxy nation is technologically less mature ~~to~~ than either the victim or attacker. The attribution is ~~in most cases~~ achieved, in most cases, after complex digital forensic work that requires massive amounts of stored traffic data and logging. Many regional I~~i~~nternet service providers on the African continent might not have ~~that~~ a rigorous enough ~~of a~~ logging and data repository for their traffic;~~,~~ measures that under normal conditions are unnecessary for conducting their daily business. The distance and potential cultural barriers are other problems that undermine the chances for attribution. If attribution is possible, it can be a slow process ~~which~~ that gives the attacker more time to create countermeasures to further hinder the efforts of the victim.

Third, it is likely that the vehicles for the attack are dismantled directly after the attack. The computers and networks that were used for the attack can have the data and traces erased beyond what can be recovered. If proxies remove the chance for correct attribution, then the fundamentals of state-to-state deterrence are no longer in place.[5]

Defusing Retribution through Proxies

Formatted: Font: Not Italic

Proxy cyber ~~-~~attacks can be a national security threat~~,~~ and create significant damage to critical infrastructure and national assets for the targeted state, if the terrorists are given the tool set and pre-attack cyber weapon design from a state actor. The targeted country, or organi~~s~~zation, could ~~assume~~ guess where the attack is coming from but attribution is not strong enough for retribution. A state engaging in retribution towards another state could face other grave unanticipated political consequences~~,~~ ~~which pose uncertainty and generate a risk avert state actor~~. The aggressor's risk is

lowered if the state actor collects vulnerabilities in the opposing state's networks, builds cyber weapons, and creates a strategy to cause disruption and destabilisz~~z~~ation in the opponent's networks – but uses a proxy to carry out the actual attack. The use of a proxy in warfare is not a new concept, and the shift from kinetic proxy warfare to cyber proxy warfare is an inevitable outcome of technological conflict. Nations in the developing world are in a position to be exploited as a proxy state due to the change of conflict environment and unprecedented routing of cyber-attacks. Several African countries have seen a drastic increase in cell phone and Internet usage, where the service providers are naturally eager to serve their customers, instead of speculating in theoretical ways ~~for~~ on the geopolitical implications of providing easy access to the Internet. If the adversary is skilled, it is more likely the attribution investigation will end with a set of spoofed, innocent actors whose digital identities have been exploited in the attack, rather than attribution to the real perpetrator.

The use of proxies undermines a clear and detailed attribution for a targeted organisz~~z~~ation or nation, which removes the opportunity for retribution and punishment. A strong suspicion would impact interstate relations, but full attribution and traceability are needed to create a case for reprisal and retaliation. Attribution can be graduated, and the level varies as to what would be accepted as an "attributed" attack. The national leadership of a targeted society can accept a lower level of tangible attribution, based on earlier intelligence reports and adversarial *modus operandi*, than the international community might demand, but it is restrained in taking action.

Conclusion

For an aggressor, the use of proxies – ,without the consent of the proxy –, is favourable in a cyber -conflict because intelligence and political goals can be reached without exposing the true origin of the attacks. Developing countries could be used as proxies, even without their knowledge and consent, by the unauthorisзed usage of these countries' information systems in the pursuit of an attack on a third country by a state-sponsored offensive cyber operation. If the purpose of the cyber -attacks are to destabilisзe a targeted society,[6] and the attack succeeds, the used proxies are likely to face consequences in their relations with foreign countries, even if the proxy was unaware of the covert activity.

A direct consequence for the country that is used as a proxy is degraded relations with the targeted state, as a consequence of the actions funnelled through their networks, and increased demands from targeted states that the proxy state secures the private and public networks within the jurisdiction of the proxy state.

~~Notes~~

[1] Jan Kallberg and Bhavani Thuraisingham, State Actors' Offensive Cyberoperations: The Disruptive Power of Systematic Cyberattacks, *IEEE IT Professional*, vol. 15, no. 3 (2013).
[2] A. Y. Keren and Keren Elazari, Internet as a CII-A framework to measure awareness in the cyber sphere, *4th International conference on cyber conflict* CYCON IEEE (2012), 1-13.

[3] David T. Fahrenkrug, Countering the offensive advantage in cyberspace: An integrated defensive strategy, *4th International conference on cyber conflict* CYCON IEEE (2012), 197-207.

[4] Paul Rexton Kan, *Drugs and contemporary warfare,* Dulles, VA: Potomac Books, 2009.

[5] Robert H. Reed, On deterrence, *Air University Review.* May-June (1975).

[6] Jan Kallberg, Bhavani Thuraisingham, and Erik Lakomaa. Societal Cyberwar Theory Applied The Disruptive Power of State Actor Aggression for Public Sector Information Security, *Proceedings from the 2013 IEEE European Intelligence and Security Informatics Conference (EISIC)*, 2013.