Cyber Warfare and Nigeria's Vulnerability

https://www.e-ir.info/2013/11/03/cyber-warfare-and-nigerias-vulnerability/

DENISE N. BAKEN, NOV 3 2013

In August 2012, Boko Haram reportedly hacked the personnel records databases of Nigeria's secret service. The individual who successfully compromised the covert-personnel data system indicated the breach was executed in the name of Boko Haram and as a response to Nigeria's handling of interactions with the group.[i] The retaliatory attack revealed the names, addresses, bank information and family members of current and former personnel assigned to the country's spy agency. The attack would not have tremendous significance in and of itself. However, it represents a substantial shift in tactics for a group whose name connotes an anti-Western stance. Until recently Boko Haram attack strategy was far from technological. However, since its association with Al Qaeda, Boko Haram has demonstrated a vastly changed approach to executing its attacks. Attacks are now more violent and reflect the markings of training by al Qaeda personnel. Given that cyber space has been part of the terrorists' warfare tool kit since 1998 when the Tamil Tigers executed a distributed denial of service attack, [ii] and al Qaeda has used the Internet as a vital communication vehicle since 1996, Boko Haram's incorporation of cyber into its arsenal is almost inevitable. More importantly though, Boko Haram's access to an individual who can execute such a successful attack is indicative of the cyber arsenal workforce capability available to any group or nation that wants to employ it. Boko Haram's tactic advancement clearly demonstrates that Nigeria and its neighboring Sahel region neighbors are ripe for exploitation as a cyber warfare hub.

Cyber warfare is experiencing a boom. The success of activities like Ghostnet, Stuxnet, Byzantine Hades, and Titan Rain has shown that the demand for such products will not slow anytime soon. Nation-states have begun to incorporate cyber warfare against opponents' cyber space attacks into their national security strategy.[iii] However, the reality is that nations executing these attacks do not always want to be identified as the perpetrators. Case in point- after a student from the University of Electronic Science and Technology of China executed a vast nation-state intrusion called 'Ghostnet', several media accounts of the attack wondered if China was involved. China denied any knowledge of the attacks and the sensitive information retrievals from 103 invaded national security databases remained unclaimed. The Chinese continued their public stance of denying culpability when a report on corporate intrusions specifically named the Chinese Peoples Liberation Army's Unit 61398. According to the report investigators traced several intrusions into United States (U.S.) corporate and government secure information technology systems to the PLA unit.

Just as China prefers a public stance of denial, so might other nations. Public response to Ghostnet and Stuxnet made it apparent nations would not always want it known that they were perpetrators of an attack. It was clear that for nation-states to continue to incorporate this new weapon, they had to accommodate the sensitive diplomatic nature of such attacks by finding an alternate approach. But we have to acknowledge that their appetites for these attacks will not diminish. If anything, they will grow. What could this mean? If we use Boko Haram as an example, we can suggest an alternate approach that leverages the chaotic political situation and burgeoning supply of talented cyber personnel within Nigeria and the Sahel. Executing attacks from this third-party cyber location, offers attack perpetrators and the cyber arms industry the ability to outsource, just as manufacturing does.[iv]

If we use the impact of improvised explosive devices on Afghanistan and Iraq as an example, Nigeria and the Sahel can offer resources for 'niggling' attacks that target nation-states with 'improvised explosive device' level attacks. These attacks would cause damage that is cumulatively significant, but individually not.[v] The costs could remain low, as the readily available workforce functions in a region with an average annual income of $1180 (U.S. dollars).

The nation-states employing this workforce will have a great cost-benefit ratio and the workforce itself will achieve success in their chosen field.[vi] While the Vice Chancellor of Osun State University is not pleased that the stated goal of computer science students was 'making money in cyber crime'[vii] the reality is perpetrators of cyber warfare can use the demographic of Nigeria and the Sahel to train recruits and execute attacks without impunity. The Sahel has an economic environment that is conducive to cyber crime activities, an exploitable sophisticated cyber highway, and an area where officials are more focused on political distractors than enforcing information communication technology regulations.

Impact of Cyber Technology

Africa is a changed region because of cyber technology (Figure 1). Areas that only had a few users a short 10-12 years ago are now experiencing extraordinary use growth that exceeds 26,000 percent. Areas such as the Sudan and Somalia experienced rates of change of 21,564% and 62,935%, respectively.[viii] Algeria has a 26,050% growth over the same time period.

Country Users 2000 Users 2012 Rate of Change Algeria 20,000 5,230,000 26050.00% Burkina Faso 10,000 518253 5082.53% Cameroon 20,000 1,006,494 4932.47% Chad 1,000 208,537 20753.70% Egypt 450,000 29,809,724 6524.38% Gambia 4,000 200057 4901.43% Kenya 200,000 12,043,735 5921.87% Libya 10,000 954,275 9442.75% Mali 18,800 414,985 2107.37% Mauritania 5,000 151163 2923.26% Niger 5,000 212480 4149.60% Nigeria 200,000 48,366,179 24083.09% Senegal 40,000 2269681 5574.20% Somalia 200 126,070 62935.00% Sudan 30,000 6,499,275 21564.25% Tunisia 100,000 4,196,564 4096.56%

Figure 1. Internet Users' Rate of Change for Selected African Countries (Source: Internet World Stats, as of 30 June 2012, http://internetworldstats.com/stats1.htm)*

Users are now aware of previously unknown opportunities because of the Internet- opportunities that offer those with an entrepreneurial spirit, an avenue out of poverty, hunger and unemployment. That avenue, cyber crime, has such a strong attraction as a career path that a 2008 survey of senior secondary students found 83% of the surveyed students agree or strongly agree that students use others' credit cards to buy merchandise, 73% strongly agree or agree that students deceive investors for money and 70% strongly agree or agree that students steal trade secrets or research documents about new products. There is also a 48.3% opinion that 'students help terrorist groups (Osama's group) to use Internet in furthering their agenda'. [ix]This acceptance of cyber crime carries over to University computer science students who have professed a desire to enter the cyber crime industry upon graduation.[x] Then there are the Yahoo boys. Young university educated men who have already entered the cyber crime industry and are now making more than their parents.[xi] With a young 'up and coming' workforce ingrained in cyber crime, cyber warfare perpetrators have a potential mercenary cadre already equipped with a psychological propensity for the employment field. In addition to this workforce with its appropriate value system, cyber crime perpetrators can benefit from safe haven attributes of; 1) a nation-state with sufficient political distracters; 2) economic environment conducive to cyber crime activities; 3) modern fiber-optic information communication infrastructure, and; 4) exploitation potential of a sophisticated cyber highway.[xii]

Nation-state with Sufficient Political Distractors

Nigeria and its Sahel neighbors have many cultural influences, particularly from a tribal perspective. In addition, there are many natural resources available for state use to contribute to the country's gross national product. But while this should be a positive, they are heavily affected by the corruption and direct disregard demonstrated by government leaders. As a result, unemployment is high, there is minimal foreign investment, and the black market runs the shadow economy with money laundering, bank fraud and identity theft running rampant. These factors contribute significantly to many of the nations in the region ranking high on the Failed State Index, from a total perspective and reflecting a high economic decline total.[xiii], [xiv]

Country Rank on 2012 Failed State Index Failed State Index Total Economic Decline Total Burkina Faso 41 87.4 7.7 Cameroon 26 93 6.5 Chad 4 108 8.3 Gambia 63 80.6 7.4 Mali 79 77.9 7.5 Mauritania 38 87.6 7.6 Niger 18 96.9 8.6 Nigeria 14 101.1 7.5 Senegal 71 79.3 6.9

Figure 2. Failed State Index 2012 Ranking with Economic Decline Indicator (Source: Fund for Peace Failed State Index 2012, http://reliefweb.int/sites/reliefweb.int/files/resources/cfsir1210-failedstatesindex2012-06p.pdf)

Economic Environment Conducive to Cyber Crime Activities

The Sahel has become a haven for Al Qaeda in the Islamic Maghreb. Illegal activity functions in the region as if political borders do not exist. Organized crime and terrorist groups attack freely, conduct business and exploit the weak controls that are enforced only on a limited basis. These business activities include drug trafficking, counterfeiting, kidnapping, blackmail, document forgery, robbery, and immigrant smuggling.[xv] There are no real economic resources and the graft and corruption severely limit any enforcement that could occur. The economic decline/failed state status of the region as a whole is ripe for additional corrupt and/or illegal behavior. Students who already participate in cyber crime activities boast of the controls they have over law enforcement officials who could/should limit their activities.[xvi] During interviews with the Yahoo boys, the young cyber criminals were confident of their hold over local officials.[xvii] They spoke of bribes to ensure no interference from law enforcement personnel.

Modern Fiber-Optic Information Communication Infrastructure

In the year 2000 only 4.5 million of Africa's one billion people were categorized as Internet users. That was a little more than .42%. However, as the continent, its resources, and potential 2050 workforce were combined to become opportunities for investors, it became apparent to these investors, and the African nations where this workforce lives, that tremendous improvements to the continent's information highway were imperative. Those improvements started with the Eastern Africa Submarine System (EASS) fiber-optic cable proposal in 2003.[xviii] Other improvements were the 2009 fiber-optic submarine cable system Seacom, the 2010 Western Africa cable system, and the 2014 projected finish of the 'connectivity' project. The continent now boasts over 15% Internet users, with some individual states experiencing much higher usage.[xix] World Bank nations that recognized this need and invested in the highway's improvements include Brazil, Russia, India and China (BRIC). South Africa joined the effort when it became a part of BRIC in 2010. With these state of the art advancements, countries like Mozambique, Tanzania, Kenya, Somalia and the Sudan enjoy connectivity via mobile telephone technology to almost anywhere in the world. The continent is now seen as an attractive foreign investment destination pursued by more than the initial chance takers. Residents of almost any state can access mobile technology, changing the definition of 'remote Africa' and the number of marginalized populations. But these same potential economy-boosting continental links also serve as the tool for cyber criminals to advance their entrepreneurial skills.

Cyber Warfare Attacks

The attacks executed by the perpetrators of Stuxnet, Ghostnet, and even Flame, were initially conceived and deployed incognito. Flame functioned for almost two years before discovery, and when found, the United States did not initially acknowledge its role. The negative international response to Flame and Ghostnet was enough for nation-states to realize that today's military strategy-international diplomacy equilibrium demands a more discreet employment of this new weapon. One that does not jeopardize current diplomatic relations or upset conventional weapons partners. The nations left vulnerable after each of these attacks also recognized that they would be at a disadvantage if they did not begin to include strategic cyber offensive and defensive operations into their national defense blueprint. While the Flame attack was directly attributed to the United States, the Ghostnet attack was never conclusively identified as China directed. The young researcher identified as Ghostnet's perpetrator was a well-known hacker who never implicated any other person or entity in the effort.

What if a nation-state employed the tactic and this type of workforce on a future attack? That is: if a nation-state

employed a third-party entity that is willing to NOT implicate the nation-state, could that nation-state successfully execute such a cyber warfare attack and not have to face the wrath of its international partners? Rafal Rohozinksi, one of the investigators of Ghostnet and cofounder of Information Warfare Monitor, has suggested that such outsourcing could become a wave of the future. Rohozinksi cites the factors that could contribute to the trend. Nations need an alternative that offers anonymity preserves current diplomatic balances and employs resources that are outside the nation's jurisdiction. According to a 2011 Harvard School of Public Health assessment Africa is expected to contribute 49% of the world's 2050 population growth.[xx] Rohozinski insists this 2050 workforce will have a demographic that is conducive to cyber crime: young, talented, from a developing nation, possessing a value system that has previously, and would in the future, support participation in or instigation of acts of cyber crime.[xxi] If Rohozinski is correct, then we have to recognize that developing nations without strong ICT rules and regulation enforcement, nations with civil unrest or nations that lack services could serve as third party locations and perpetrator source.

The perpetrator source could easily begin with the University students who have professed a desire to work in the cyber crime industry. Taken together these factors make Africa attractive to almost any investor, especially any who inhabit the shadowy world of cyber crime. To hacking investors the limited resources needed to establish a presence is particularly inviting. There is already an experienced cyber crime workforce, a reduced enforcement of ICT rules and regulations, a strong malware history and an economic environment that makes the potential very attractive. As a business venture, there are few negatives.

Which Cyber Crimes?

Criminal use of the region's Information Highway already include electronic mail scams, scam letters that range from the purchase of real estate, disbursement of money from wills, to the sale of crude oil at below market prices. Communication usually occurs through electronic message via fax, e-mail or cell phone. Verification is difficult so victims ultimately pay the fees without evidence to validate the claim of the perpetrator. While these types of cyber crime are perpetrated on a large scale in countries like Nigeria, the crimes themselves are not target specific. The perpetrators initiate several scams at a time so that the perpetrator financially benefits, on average, from some, if not all, of the scams. No one victim is regarded as the single important prey.

Given the ideal conditions the region offers for third party cyber warfare attacks, several questions must be answered for national security strategists to understand the threat they could potentially face: would these same Nigerian or Sahel region cyber crime perpetrators initiate their perfected scams for another entity? Are they willing to expand their skill set and advance into target specific entities? Finally, if they were willing to initiate target specific entities, would they execute an attack on infrastructure? If they initiate the crime, is there a limit to the type of crimes they will launch?

There is already a perception/acceptance of students who "steal" trade secrets, research documents or supplier's agreements. If the Boko Haram attack is an indication, they very well may be. An almost unencumbered access to high quality information communication technology, combined with the computer literate young of 2050, make it wise for potential target nations to understand the threat this region could represent for them. They must accept the reality that the opportunity this new industry offers the Sahel's employment-opportunity-constrained workforce, and the potential to earn a living far above the current $1180 (U.S dollars) annual income, make the Sahel's attractiveness as a cyber warfare third-party haven almost irresistible.[xxii]

Conclusion

The Sahel is already home to a variety of illicit activities, and adding cyber warfare to that list is not far fetched. Nation-states could benefit from expanding their repertoire of weapons, terrorist actors could include it in their arsenal against the West, and both would achieve their goals and objectives without significant infrastructure modifications. This could redefine cyber crime if both the nation-state and the terrorist actors, reconcile their value system by incorporating this approach to expanding their warfare arsenal.

These perpetrators of ill intent (whether nation-state or terrorist actor) recognize that, in today's world, their victims do not have the option of 'no presence on the web'. They can, therefore, inflict damage, pinpoint attacks, and execute attacks without significant cost. Their potential victims must therefore learn how to counter this attack approach while minimizing the negative impact on the already fragile economies of the Sahel and, even, Nigeria.

The nations in the region, themselves, have to also include this consideration as they develop their law enforcement approach to information communication technology regulation enforcement. Each nation already has shadow economies from the illicit crime and that economy feeds, houses, and clothes many of its citizens. The governments of the area have to form a coalition with investing countries and identify alternates for these potential "failed state mercenaries" and their robust cyber warfare attack tools. We underestimated Boko Haram in the past. We should not underestimate the bellwether Boko Haram's cyber attack may represent.

—

Denise N. Baken *is the president of Shield Analysis Technology and faculty member at George Mason University. This article is part of e-IR's Edited Collection 'Boko Haram: The Anatomy of a Crisis'.*

[i] Bashir Adigun, "AP Exclusive: Nigeria Secret Police Details Leaked," *Salon*, August 30, 2012, http://www.salon.com/2012/08/30/ap_exclusive_nigeria_secret_police_details_leaked/.

[ii] Dorothy Denning, "Cyberterrorism – Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives," *Georgetown University*, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

[iii] Elinor Mills, "Report: Countries Prepping for Cyberwar," *CNN*, November 17, 2009, http://articles.cnn.com/2009-11-17/tech/cnet.cyberwar.internet_1_south-korea-cyberwarfare-cyberattack?_s=PM:TECH.

[iv] Denise Baken and Ioannis Mantzikos, "Cyberspace Improvised Explosive Device and the Failed State Catapult-The Strategic Symbiotic Relationship Failed State Status Offers Nation-State Cyberwarfare Arsenals," in *New-Old Salafi/Al Qaeda Threats* (presented at the 5th Annual ASMEA Conference-History and the "New" Middle East and Africa, Washington, DC: Association fro the Study of the Middle East and Africa, 2012).

[v] Ibid.

[vi] Shuaib Shuaib, "allAfrica.com: Nigeria: Cyber Crime, Our Biggest Problem – VC," news, *allAfrica.com*, September 1, 2010, http://allafrica.com/stories/201009010416.html.

[vii] Baken and Mantzikos, "Cyberspace Improvised Explosive Device and the Failed State Catapult-The Strategic Symbiotic Relationship Failed State Status Offers Nation-State Cyberwarfare Arsenals."

[viii] "Africa Internet Usage, Facebook and Population Statistics," *Internet World Stats: Usage and Population Statistics*, June 30, 2012, http://internetworldstats.com/stats1.htm.

[ix] Olugbenga Adedayo, "Secondary School Students' Perceptions of Incdences of Internet Crimes Among School Age Children in Oyo and Ondo States, Nigeria (dissertation)" (University of Ibadan, Nigeria, 2008), http://www.kaspersky.com/images/secondary_school_students_perceptions_of_incidences_of_internet_crimes_among_school_age_children_in_oyo_and_on-10-75860.pdf.

[x] Shuaib, "allAfrica.com: Nigeria: Cyber Crime, Our Biggest Problem – VC."

[xi] Baken and Mantzikos, "Cyberspace Improvised Explosive Device and the Failed State Catapult-The Strategic Symbiotic Relationship Failed State Status Offers Nation-State Cyberwarfare Arsenals."

[xii] Ibid.

[xiii] The Failed State Index rates several indicators, one of which is economic decline. The maximum number a country receive for any indicator is 10.

[xiv] "The Failed States Index 2012 Interactive Grid," *FFP The Fund for Peace*, June 18, 2012, http://www.fundforpeace.org/global/?q=fsi-grid2012.

[xv] Baken and Mantzikos, "Cyberspace Improvised Explosive Device and the Failed State Catapult-The Strategic Symbiotic Relationship Failed State Status Offers Nation-State Cyberwarfare Arsenals."

[xvi] Adebusuyi Adeniran, "The Internet and Emergence of Yahooboys sub-Culture in Nigeria," *International Journal of Cyber Criminology* 2, no. 2 (December 2008): 368–381.

[xvii] Ibid.

[xviii] Osman Dahir Osman, "Submarine Fiber Optic Route to Somalia," *Hiiraan Online*, September 27, 2007, http://www.hiiraan.com/news2/2007/sept/submarine_fiber_optic_route_to_somalia.aspx.

[xix] "Africa Internet Usage, Facebook and Population Statistics."

[xx] Hao Li, "World Population to Top 9 Billion by 2050, 49% Growth from Africa," *International Business Times*, July 29, 2011, http://www.ibtimes.com/world-population-top-9-billion-2050-49-growth-africa-820105.

[xxi] *Panel on Cyber Crime*.

[xxii] "UNICEF – At a Glance: Nigeria – Statistics," *UNICEF*, accessed February 20, 2013, http://www.unicef.org/infobycountry/nigeria_statistics.html.

About the author:

Denise N. Baken is the president of Shield Analysis Technology and faculty member at George Mason University