

The Evolution of a Sub-National Entity in Cyberspace: The Rise of the Cyber Cell

Cyber al Qaeda

WILL GRAGIDO

CISSP CISA NSA-IAM/IEM

May 4, 2010

Evolution of Sub-National Entity in Cyber: Cyber Qaeda

“Nothing that is so is so.”

William Shakespeare — Twelfth Night, Act 4, scene 1

When the Improbable Becomes the Inarguably Probable

One should never take anything at face value. I realize this sounds pessimistic however we live in a world in which the improbable often becomes the inarguably probable. At times this occurs with a vengeance. Often, it occurs with malicious intent and catches us off guard in a state of complacency where we are vulnerable; easy targets for those with nefarious intent. By nature I am not one for taking anything at face value. I tend to resort to natural states of information collection, digestion, analysis and decision-making; it's just who I am. It's part of my make-up as an analyst. I've learned over the years that to do otherwise, to become too comfortable, too at ease, too leisurely can have adverse consequences. Yet one cannot live in a heightened state of awareness at all times and as such advanced means for dealing achieving balance should be sought. I don't believe that I am alone in this nor do I believe that vigilance is the stark equivalent of paranoia. Vigilance and attention to detail can aid one (provided one is open to it), can aid in avoiding what can amount to a great deal of trouble. This is true in all aspects of life; attention to detail is critical, it can mean the difference between life and death. As a result, our industry is no exception to this rule. As Aristotle said so eloquently “the probable is what usually happens”; I agree with him. The probable is what usually and almost always does happen.

Through the Looking Glass

For this reason and those that follow, I would like to expand upon while further exploring these ideas. I think it is extremely important to do so especially in the wake of the so-called advanced persistent threat (APT) attack code named ‘Aurora’ by McAfee and Google. It should be noted that I believe emphatically in the realities associated with the advanced attacks (state sponsored, sub-national or cyber criminal in origin). Advanced persistent threats (APTs) are real but as I've written in previous works, they are merely a subset of more advanced compromises; compromises which are better understood in more comprehensive taxonomies such as the Subversive Multi-vector Threat (SMT). Without reliving the events surrounding the Google China incident or the data points associated with it (many of which over time changed and were found to be of questionable relevance, accuracy and authenticity), it is important to note that many eyes, ears, hearts and minds were directed and focused upon ‘Aurora’—regardless of its authenticity, my assertion is that many other more diligently focused cyber actors and threats (state and sub-nationally sponsored – criminally, politically, philosophically, theologically motivated; foreign or domestic), may have been missed; unintentionally allowed to slip through the cracks and crevices alike of our defenses (many of which are the result of our own device), due to the energy having been spent in investigating it and all things China borne. This of course begs the questions that while many organizations operate under the belief that though they were not afflicted by this threat or those like it, how many *are* and *were* truly impacted? How many will be impacted to come? There is danger in operating under the delusion that one is impregnable to such threats. Safety and security come at a price. This price is derived from the valuation an organization places on its assets versus the cost to secure; it's a simple proposition yet one which seems to eclipse many. Bruce Schneier wrote a nice piece back in 2008 on the psychology of security. I found it interesting, as I'm a student of psychology working towards a master degree and have read ample texts and papers on the matter. Put plainly Schneier focuses on the distinction between *feeling* secure and *being* secure something is often misunderstood (unless addressed in context) and often underestimated in terms of the impact associated with either. Schneier's point is one that rings true with respect to this in my opinion.

Purpose In Writing

Before going any further I think it is both appropriate and responsible to clearly articulate the nature and purpose of this article. This article is not being written as an expose or in depth analysis piece on al Qaeda as a sub-national terror organization, acting out its Salafist jihadi agenda. Nor is it meant to be a thorough examination of all seven prescribed stages of jihad (provided below as a point of reference), as Fouad Hussein (a Jordanian journalist who spent time in prison with Abu Musab al-Zarqawi,) provides in his book *Al-Zarqawi – al-jil aljadid lil-Qa'idah* (Qaeda's Second Generation).

Figure: Seven Prescribed Stages of Jihad Over a 20 year Period

1. Phase One: "Awakening"
2. Phase Two: "Opening of Eyes"
3. Phase Three: "Arising and Standing Up"
4. Phase Four: "The Down Fall and Collapse"
5. Phase Five: "Creation and Appointment of the Islamic State or Caliphate"
6. Phase Six: "Total Confrontation"
7. Phase Seven: "Definitive Victory"

No, though there exists some speculation as to the order (in terms of sequence), there seems to be little speculation concerning the purpose, directives and areas of priority represented by Hussein for subversive, violent action. Equally important is the disparity of ideologies represented amongst the various factions of Salafist jihadists. Failure to understand and comprehend this can result in bitter ends. No, my purpose in writing this is to bring light on the potential rapid adoption of traditional criminal activity by al Qaeda cells and operators in order to subsidize any and / or all of their activities. Specifically, my purpose extends to the logical adoption and entre into cyber criminal activity by al Qaeda in order to realize profit to support their ends.

My interest in al Qaeda stems largely from their involvement the attacks of September 11, 2001, though my experience with Salafist Jihadi Organizations dates back to the 1990s and my time in the United States Marine Corps. Recently I've read several papers and articles that have given me cause to the reconsider something which I had put on the proverbial 'back burner' for quite sometime: *what is the likelihood of al Qaeda cells and operatives, in their currently organizational state, not only engaging traditional criminal activity (a theory which I hold and am working on for another people which suggests a natural evolution of effort in traditional criminal organizations toward cyber activity and, where and when 'appropriate' -- based on need, the adoption of traditional criminal activity or alignment with traditional criminals to subsidize their activities)*. I see this as being probable as opposed to being improbable. It is neither hard to conceptualize nor believe given the level of sophistication, knowledge, training and resources which al Qaeda, its cells and other organizations like it the world over possess.

Infiltrating the Mind of Cells and their Operators

Al Qaeda is not the only sub-national organization in the world to use and or employ a cell model to and including 'sleeper' cells. No one should labor under this mindset. However for the purpose of this paper it is the primary focus of my attention. It should be noted that there are terrorist organizations the world over all of which espouse their own rhetoric and beliefs (some Salafist jihadi, some anti-Marxist, some Christian anti-Islamist, some Jewish anti-Islamist, some Christian Catholic anti-Protestant, some Christian Protestant anti-Catholic etc.). However in order to fully grasp the mindset of the Salafist jihadi mindset, one must first be able to fully appreciate and comprehend the ties which exist today, between what the Salafist jihadi considers his 'sacred past' and the modern world.

In doing we can achieve an understanding of them the likes of which Dr. Magnus Ranstorp pointed out in his paper *The Virtual Sanctuary of al-Qaeda and Terrorism in an Age of Globalization*. As Dr. Ranstorp suggested it is critical to note these relationships and how the rise of globalization has and will continue to impact advanced terrorism in the 21st century. Though Dr. Ranstorp is not the first party to make this correlation, he articulates an extremely valuable point and that point is that the result of a new era in globalized economics will see a new standard being brought to bear in activity traditionally associated with sub-national entities such as al Qaeda. This new standard sees the rise of a new, adaptable, and complex form of 'networked' asymmetric adversary come to life. One, which knows only the bounds of its skill sets and resources. Mastering this understanding (of Salafist jihadists) will enable the analyst to develop a more sophisticated understanding of the jihadi mindset, their views on technology and on Occidentalism as a whole.

I'm Not Young Enough To Know Everything, But There Are Some Things I Don't Doubt

Oscar Wilde is credited with saying he wasn't young enough to know everything a statement many of us would do well to remember. I don't believe I'm young enough to know everything either, a realization which I came to honestly through many years of experiences. As a result, I tend to believe that you should never discount what you cannot prove regardless of how unlikely it may seem to you. The improbable is often discounted entirely while at times the impossible (or seemingly so), is believed entirely. It is a strange yet wonderfully confusing phenomena. This piece was conceived with the idea of al Qaeda 's entry into criminal activity being completely probable and as such their subsequent entry into cyber crime a logical conclusion. I believe I am not alone in this belief and found that at least one recent article published by Forbes magazine in February of 2010 described what I found to be both intriguing and of corollary value to my point. In this [article](#), al Qaeda (an organization which likely needs no introduction in the 2010), was said to be on the verge of a financial crisis leading toward bankruptcy. Al Qaeda as we know is an organization which has been described as something of a hybrid; a midway point between a religious sect and a medieval military order not unlike the Knights Templar of medieval Europe. It is an organization subject to a great deal of debate and conjecture. For example, Dr. Magnus Ranstorp is often quoted as stating that there is such a mature degree of uncertainty regarding al Qaeda that its very essence is often discussed in ideological terms, socio-philosophical terms and, to a lesser extent simply as a darknet; a virtual network replete with the blindly faithful and willing masses, their handlers, and those willing to architect chaos, death and destruction to further their cause. I believe that given the current state of the organization there is likely some truth to all of these perceptions of the organization as it is seated today.

This article however, deals with the solvency of al Qaeda, specifically whether or not it as an organization is in effect bankrupt, and as a result if it's operating model and philosophy have changed dramatically as a result. The answer is not a simple "yes" or "no" but rather something more complex. Yes, it appears that al Qaeda is experiencing serious financial trouble if in fact they are not bankrupt. The result of their state is that their operating model has in fact changed. It has changed dramatically and taken them into areas that they were traditionally not a part of. In order to appreciate the full gravity of these turns of events one must take into consideration the following:

- In 2000 – 2001 al Qaeda had an annual operating budget of approximately \$30 million USD
- In 2009 – 2010 al Qaeda is on the verge of insolvency

Consider those facts for a moment. In 2001, the annual operating budget of al Qaeda, the infamous global terror organization – not an enterprise organization conducting commerce in some near or far corner of the world, but a terrorist organization, had an annual operating budget of \$30 million USD, a figure which equated the 2005 military spend of the African nation of Togo! Fast forward nine years and al Qaeda's existence is dubious at best largely due to pressure exerted by the U.S. government to free assets and accounts belonging to al Qaeda sympathizers and supporters. These accounts, many if not all, belong to fund raising agents or front organizations which in turn launder the funds and subsequently forward them to al Qaeda for use at its discretion in order to perpetuate its goals. The result of this attack on the financial health of al Qaeda is ongoing and has seen the organization adapt (as mentioned previously), in order to continue operating. One of the key adaptations the organization has undergone is a fundamental departure from a well-structured, hierarchical organization to a decentralized one where the cell and operator have more discretionary authority. Working and operating as a confederation of cells – cells who's leaders assume the responsibility for target acquisition, tactics and strategy, in addition to the generation of funds, al Qaeda's new manifestation has proven both challenging and unsettling to analysts the world over.

New activities undertaken by these cells have included (but not been limited to):

- Involvement in the international drug trafficking trade from South America to Europe via North Africa
- Involvement with violent, organized crime syndicates working and operating in within the Indian Subcontinent and South Central Asia
 - Drugs
 - Prostitution
 - Contract Killing
 - Extortion

After reading the Forbes article and conducting more diverse and comprehensive research, it occurred to me that the only activity which this new breed of al Qaeda had not overtly undertaken for profit was the one which seemed to me to be a natural extension of their pre-existent skills set: cyber crime. Whether they were to do so on their own behalf for their own express profit or acting as a third party competing for business within the underground would remain to be seen but seems like a natural probability; an inevitability given the circumstances they are facing. For example, we know for a fact that for over ten years al Qaeda operatives have been actively probing and enumerating elements of American infrastructure remotely (for example spoofing an address in India, hopping from India to Indo-China, to Saudi Arabia with a destination of a network infrastructure in California). We also know they possess the capability and knowledge to actively engage in this level of reconnaissance and likely much more. So is it reasonable to believe that they will endeavor into more lucrative activity that poses a more advantageous 'risk reward' proposition? My belief is that if they are not already doing so, they will, as there is great potential to earn a great deal of money. Likely, this will be done using fronts and aliases in order to ensure operations in the underground run smoothly as the goal would be to minimize risk while maximizing profits.