A Research Proposal into the National Security Perils of Hacktivism

Carter Matherly

A Research Proposal

Carter Matherly

2011
I. Introduction:

On December sixth 2010 the words, “Fire now,” echoed throughout Twitter and cyberspace (Cohen, 2011). Almost inexplicitly out of the ether a rag tag group of internet pranksters came together as a coherent, driven, and dangerous force. They attacked MasterCard, Visa, and PayPal simultaneously. The banks fought back valiantly but were no match for the size of the attack and fell, however briefly, in face of the onslaught (BBC, 2010).

The group that calls itself Anonymous, originally known for its antics defacing websites and harassing Scientology, found something to fight for. Wikileaks, the self-proclaimed whistleblower website, was without question an outright beneficiary of the attack. Wikileaks achieved a high level of publicity when it uploaded thousands of classified documents to the internet. However, the site itself is not what Anonymous was fighting for. Defending freedom was the call they answered. Freedom of the internet, information, basic human rights, and speech were the real beneficiaries in their eyes.

Today this very large and very powerful group of vigilante hackers lurks on the edge of the internet. There is no leader, no membership card, or test to become a member of Anonymous (Lillington, 2011). The execution of these attacks was no small feat orchestrated by a few rouge computer owners, but required great skill by a very large number of professional hackers working together at immense risk to themselves. The group feels it is their duty to police the internet, attacking those that they believe stifle the freedom of speech (Lillington, 2011).

Normally America has had the great fortune to recognize and identify its adversaries before they are able to strike. Why then would we turn a blind eye to this potential threat? This
vigilante ‘hacktivist’ group poses a severe threat to American National Security based on conflicting ideological precepts, both hidden and public agendas, an increased dependency on technology and application thereof, coupled with potential noise from vested third parties.

Should America be concerned with this rouge group of hackers? As the US found out in the first gulf war they are not impervious to hackers. Before the first assault on Iraq highly classified strategic documents were stolen from DoD computers by Dutch hackers (James G. Barr, 2004). Luckily the Iraqi government declined to purchase the information, suspecting it was a hoax.

II. Literature Review:

There is ample work highlighting the danger hackers pose to individuals and corporations. There is also a copious amount of work discussing numerous aspects of National Security. However the current state of scholarly work dedicated to the cyber strength and vulnerability of our National Security is alarmingly scarce.

As discussed above James G. Barr (2004) starts his research out promisingly enough. He details a prime incident where organized hackers successfully stole secret documents from the US with the intent to sell them to the Iraqi government for exploitation during a conflict. However after this opening incident Barr moves on without skipping a beat to the priorities and legal impacts a CFO should consider when defending their company from cybercrime. This was the closest any researcher came to bringing cybercrime in tune with National Security.

A few other authors offered valuable research and insight into one or the other of our two subjects, National Security and Anonymous. Vaughn (2010) wrote a very impressive and
detailed thesis that presents in-depth analyses of the linguistic construction and nuances of the online community. She provides some background and amplifying information on Anonymous. This information is invaluable when pursuing quantitative data for later analysis. Yet there is no mention of National Security or any potential threat posed by the group.

Fran Howarth (2010) presents a lot of statical data regarding hackers and attacks throughout 2008 and 2009. Her work pulls statical data from a number of sources, but most paramount of these is Symantec’s annual cyber security report. This annual report details key trends in security breaches and incidents in the cyber domain.

The report offers some insight into who was likely to be attacked as well as how they would be attacked. The report showed that in the first half of 2009 social web sites, such as Facebook, was the number one target, receiving 19% of all attacks. The report noted that financial firms had been in the top spot in previous annual reports but rested at fifth place with only five percent of all attacks. Government agencies also fell in ranking, going from second to a four way tie for third with 12% of attacks.

Even though she analyzed a large amount of statical data and a few comparisons of the provided material her work is rather short and highlights only processed numbers. There is no attempt to reason or form a theory for increases and declines. She does point out that of the top two motivations driving attacks were to either deface a website or attempt to gain sensitive data. The study falls short of defining what was considered ‘sensitive data’ and does not draw any possible relation to National Security.

There is a marked absence of scholarly work directly addressing the hacker group Anonymous and any potential threat they pose to not only the US, but industry, private firms,
and even individuals. Even more startling is the lack of work directly addressing National Security with regards to cyber-terrorism (or hacking). There is plenty of work addressing either National Security or cybercrime in some form or another. Yet the existing literature does not directly address hackers, let alone Anonymous, as potential threats to National Security. The concentration of the proposed research will attempt to identify troubles within National Security as well as conflicts that have caused Anonymous to take offensive action against varying establishments.

III. Theoretical Framework

Through a mixed method research approach this study will detail how Anonymous is a threat to National Security. Utilizing existing research and credible documentation of Anonymous the study will start by outlining the structure, size and scope of Anonymous. The study will establish a base of quantitative data that will be analyzed in order to test the hypothesis. The majority of the research will be spent deriving information directly from the group’s activities and published National Policy. Anonymous’ attacks give a wealth of information that can be exploited to better understand and then predict future attacks before they happen. By comparing Anonymous’ ideals, past actions, hierarchy, structure, and social goals to that of America’s National Security the proposed research will be able identify potential threats to the latter.
IV. Research Design and Methods:

The United States has already quantified its standards as well as its priorities for National Security (Department Of Defense, 2006). These standards will provide the basis for determining what the US deems as potential threats. This, combined with Anonymous’ previous actions, will allow us to quantifiably state whether or not the hacker group poses a threat to national Security.

One of the greatest limitations of the qualitative portion of this research is the amount of information available on Anonymous. Due to the lack of quantitative information a portion of the study will be devoted to scrutinizing information available on Anonymous through their actions, other research, press releases, and chat sessions amongst its members.

Collecting and sorting relevant quantitative information on National Security will be much simpler. The United States Department of Defense publishes numerous documents every year detailing National Security priorities and actions. It is from these official documents and policy written on currently accepted threats that will help to form the quantitative basis for National Security.

Additional quantitative data will be gathered through two different interview processes. One will concentrate on National Security professionals and the other on members of Anonymous. Participants will be solicited through professional and appropriately related web sites as well as forums. Members of each demographic will be told they are participating in a study investigating the current state of cyber security. To avoid leading the results in favor of the current hypothesis or research question these pieces of information will not be presented during
the interviews. Rather, questions about threats and potential victims will be left vague allowing
participants to draw their own conclusions based on their own professional experience and
opinions.

After a definitive analysis of Anonymous and United States National Security policy has
been established and analyzed for relevant quantitative information the study can progress
towards testing the hypothesis. Utilizing LexisNexis, Google Scholar, and EBSCO suite the
study will draw information gathered in previous studies and articles on National Security,
threats, cybercrime, hacking groups/individuals, and noted threats to National Security. An
example of a documented threat to National Security would be Al Qaeda (Department of
Defense, 2006). The recognized threat that these additional groups pose to National Security will
help justify how Anonymous poses a similar, if not more severe, threat.

The summation of the above research will result in a copious amount of raw data for
analysis. Before the data can be analyzed it must first be categorized. The data will be broken up
into the following major categories; Perceptions, Reality, Shortfalls, and Conclusion.

Perceptions will then be divided into several sub categories that will allow for easy
comparison. In these sub categories of data the study will examine how National Security and
Anonymous each view themselves. This includes their self-image of structure, purpose, and their
own overall security. This section will also highlight what each view as potential threats to their
own security. This data will be derived from interviews and information published or approved
by the appropriate organization.
The Reality topic will take a more in-depth look into what the data has to say about the organizations. This section will rely on reported data as well as the actual actions and precedents set forth by both National Security and Anonymous. Each organization will have a full profile derived from the data in this section. The profiles will address the same main topics addressed in the Perceptions section; structure, purpose, and overall level security.

As we all know a person’s self-image usually differs from how everyone else sees them. The Shortfalls section will compare the Perceptions and Reality section with each other. As indicated by the title of this section the study will work to identify shortfalls stemming from the organizations perception of self-image and how that differs from the profile compiled in the Reality section.

Conclusion is the final section in the processing of the collected raw data. Here the study will draw on the three previous sections and answer the overall question; does Anonymous pose a serious threat to American National Security? With the given structure of the previous sections any bias towards a positive or negative answer should be eliminated.

The summation of this information will allow scholars to indiscriminately view Anonymous as a potential threat to National Security. The study will present information that will not only support the hypothesis, but will highlight data that may not support it as well. By rendering information in this fashion the study will provide valid and justifiable reasoning for the overall conclusion.
Reference List.


Cohen, Noam (2010) “Pranksters find a cause in defending WikiLeaks; Group called Anonymous focuses on freedom of Internet in latest attacks” The International Herald Tribune, December 11, 2010 Saturday


Vegh, Sandor (2005) “The media’s portrayal of hacking, hackers, and hacktivism before and after September 11” First Monday, volume 10, number 2 (February 2005)

Prichard, Janet J. and MacDonald Laurie E. (2004) “Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks” Bryant University, Smithfield, RI, USA

Lillington, Karlin 2011 “Time to talk: Anonymous speaks out” The Irish Times, January 24, 2011 Monday