2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

Determining Extremist Organisations' Likelihood of Conducting Cyber Attacks

Steve S. Sin
National Consortium for the Study of Terrorism and Responses to Terrorism (START)
University of Maryland
College Park, MD, USA
sinss@umd.edu

Elvis Asiamah*
National Consortium for the Study of Terrorism and Responses to Terrorism (START)
University of Maryland
College Park, MD, USA
easiamah@mix.wvu.edu

Laura A. Blackerby*
School of International Service
American University
Washington, D.C., USA
lauraablackerby@gmail.com

Rhyner Washburn*
The Graduate School: Cyber security
University of Maryland, Baltimore County
Baltimore, MD, USA
rhynerwashburn@gmail.com

Abstract: The 2007 cyber attacks against Estonia were a prime example of how hackers can operate within a nation's cyber domain. Looking at today's cyber landscape, it would seem that the tools needed for an offensive cyber operational capability are readily available to a properly motivated extremist organisation. Reports and articles about hacking and cyber security from think tanks and popular publications focused on technology and business tend to reinforce such a perception. In the nexus of cyber and physical and especially in the context terrorism, given the availability of offensive cyber capability, it is unclear why more extremist organisations are not engaging in offensive cyber operations. To investigate this anomaly this study employed a structured expert elicitation to identify a set of variables that would assist in determining an extremist organisation's likelihood of choosing to engage in cyber attacks. The results revealed that while there are points of convergence as well as extreme divergences in the assessment, *level of Internet presence, access to human resources*, and *human resource available (internally to the organisation)* were assessed to have the most explanatory power for determining an extremist organisation's likelihood for engaging in offensive cyber operations.

Keywords: *offensive cyber capabilities, cyber physical nexus, future threat, extremist organisation, organisational characteristics*

* Second through fourth authors listed in alphabetical order

Any opinions, findings, or conclusions presented here are solely the authors' and are not representative of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) or the University of Maryland.

1. INTRODUCTION

The transformation seen in the cyber landscape over the past decade has been both a blessing and a curse. Humanity has benefited from this evolution, but the current cyber threat-scape has many officials worried about the potential of extremist organisations conducting offensive operations in the cyber domain. The tools needed for offensive cyber operations seem to be readily available to highly motivated individuals or extremist organisations. 'Criminal activities in cyberspace are increasingly facilitated by burgeoning black markets for both tools (e.g., exploit kits) and take (e.g., credit card information) …' (Ablon, Libicki and Golay, 2014). 'Just as you can use Taskrabbit to find someone to fix your kitchen cabinets, so too can you find a hacker to perform digital espionage or destruction. Hackers are now offering their services online to the highest bidder' (Weissman, 2015). In the nexus of cyber and physical and especially in the context of terrorism, given the availability of offensive cyber capability, it is unclear why more extremist organisations are not engaging in, or attempting to engage in, offensive cyber operations either as a standalone or as a part of a comprehensive attack methodology?

There has been quite a bit of discussion about terrorist organisations' use of the Internet for recruitment and propaganda purposes, and there has been, of late, concern about the degree of cyber threat posed by extremist groups such as Islamic State (see, for example, Perlroth, 2015). Despite burgeoning discussions and literature on offensive cyber activities and the future of cyber security, these discussions and the literature have all too often been restricted to the technical domain. The extant literature, especially, tends to overlook or only pay scant attention to the fact that there is an individual or a group of individuals making the decision as to whether or not if their organisation will engage in offensive cyber operations, or will develop such a capability.

Since there are no preceding studies that systematically explore this issue, or that examine the human or organisational aspects of offensive cyber operations in the context of terrorism, research is needed to determine what characteristics make an extremist organisation more likely to engage in offensive cyber operations. We decided to take a three-phased approach to examining the issue. In Phase I, we conducted a structured expert elicitation to identify potential explanatory variables against which to collect data in Phase II of the research. In Phase II, we will construct a violent extremist organisation dataset that includes the cyber relevant variables identified in Phase I to empirically determine the organisational characteristics that make violent extremist organisations more likely to engage in offensive cyber operations. Finally, using the results of Phase II, we will conduct further research to elucidate the possible answers to the overall research question in Phase III – an empirical examination of why only a limited number of extremist organisations have engaged in offensive cyber operations thus far, as well as a forecast of the potential future threat-scape.

This paper, a product of Phase I of the research, discusses the results of the expert elicitation and provides some conclusions and implications. The remainder of this paper is organised into four sections. Firstly, it presents a summary review of literature that focuses on why extremist organisations have not been conducting offensive cyber operations. Secondly, research design

and methodology are discussed. Thirdly, the results of the structured expert elicitation are explicated, and finally, conclusions and implications are presented.

2. SUMMARY REVIEW OF RELEVANT LITERATURE

The largest difference between an offensive cyber operation and a conventional offensive military or terrorist operation is the domain where these operations take place. Offensive cyber operations are executed in (and through) the cyber domain, while conventional offensive military or terrorist operations are performed in the physical domain. While this distinction may seem like a gross simplification, the fact of the matter is that this difference in operational domains is what makes offensive cyber operations one of the most challenging (perhaps even the most challenging) national security issues of today and the future.

Scholars suggest that as conventional counter-terrorism measures against extremist organisations continue to increase, more groups will turn to the Internet as the next frontier for conducting offensive operations. The high level of anonymity that an individual or a group can maintain while operating in cyberspace, making law enforcement efforts and interdiction very difficult, as well as the relative low cost of such operations, are thought to be the primary reasons for this potential strategic shift.

Most aspects of modern life rely on Internet use and this nearly ubiquitous connectivity amplifies the opportunities for malicious actors to engage in cyber attacks against nearly anyone or anything from anywhere in the world while remaining anonymous (Cox, 2015; M86 Security Labs, 2010; Pawlak and Wendling, 2013). Aside from the near ubiquitous connectivity, the ease of purchasing cyber weapons, the support from malware developers and the broader black hat community, the relatively low skill level needed to become a 'hacker', and the heuristic nature of hacking, have all been assessed as primary reasons that have contributed to the increase in malicious actors' operations in cyberspace (Greenberg, 2012; Fossi, et al., 2008; Goncharov, 2013; Fortinet, 2012; Pawlak and Wendling, 2013; Peterson, 2013; Zhang, Jha, and Raghunathan, 2014).

Despite the apparent advantages the cyber domain affords various state and non-state actors to conduct nefarious activities in anonymity, it would appear (at least based on open source information), that large extremist organisations such as the Haqqani Network, al-Qaeda, and the Islamic State[1] have had little or no interest in conducting offensive cyber operations in earnest. This seems to be an apparent incongruity; if the cyber domain does indeed afford such advantages, why have extremist organisations not invested in using it much more than they have thus far? The literature addressing this issue largely refers to the mismatch between the effects of cyber operation and the overall goals of the extremist organisation as the primary barrier for the extremist organisation's engagement in offensive cyber operations.

1 Islamic State may be exploring the potential of incorporating offensive cyber operations into its overall attack methodology. According to Caitlin Durkovich, Assistant Secretary for Infrastructure Protection of the U.S. Department of Homeland Security, the Islamic State has been attempting to 'hack' into the U.S. electric grid (Pagliery, 2015). George Osborne, Chancellor of the Exchequer of the U.K., also purported that Islamic State is attempting to launch cyber attacks aimed at Britain's airports, hospitals, and the electricity supply (Bloom, 2015). Other reports seem to indicate that Islamic State does indeed have some very rudimentary cyber capabilities, but it has not made cyber capabilities or cyber operations one of its core goals (Perlroth, 2015).

The extant literature, drawing on the extensive terrorism literature, calls attention to the three broad goals that need to be met in order for an attack to be considered a success for extremist organisations: 1) incitement of fear on a massive scale that will reverberate beyond the initial attack; 2) satisfaction of a strategic political or religious objective; and 3) visual destruction in order to propagate fear (Archer, 2014; Cox, 2015; Kenney, 2015). While an extremist organisation could achieve the first two goals described above through a cyber attack relatively easily, attaining a visual destruction is exceptionally difficult through the cyber domain. Furthermore, to date, cyber attacks have been primarily used to disrupt rather than destroy, one of the core elements of a terrorist attack (Cox 2015).

The reason why cyber attacks have been used primarily for disruption rather than for destruction thus far can be attributed to the design of the cyber weapons themselves, as well as to the perpetrators' preferred outcomes from cyber attacks. First, typical cyber weapons, with the primary exception being Stuxnet and its variants, do not generally cause physical destruction since they are primarily designed to infiltrate a system to gather intelligence. Second, in the context of cyber attacks, disruption of a Wi-Fi network, electric grid, or database firewall is far preferable to destroying it, since disruption allows the perpetrators to move through the system unchecked and leave a backdoor so that they can return to the system in the future (Kenney, 2015; M86 Security Labs, 2010; NTT Group, 2015; Greenberg, 2012; Peterson, 2013; Zhang, Jha, and Raghunathan, 2014). Ponagi, et al. (2012) has also suggested that cyber weapons have a specific second-order-effect of psychological function, be it to spread confusion; foment distrust within the users of the targeted system; deceive; or distract so that the attacker can move through the system freely to obtain their goal. The assessment of the extant literature is that if a cyber attack were used to destroy rather than disrupt, quite apart from the technical challenge, the attacker would lose all the benefits that could be gained through cyber disruption.

Other factors that could serve as barriers to the extremist organisations' use of offensive cyber operation are attribution, cost, and sustainability. A central tenant of conducting an offensive cyber operation is to make sure the attack cannot be traced back to the originator. Non-attribution is vital because this allows the perpetrators to work freely with relatively low fear of being discovered or interdicted (Archer, 2014; Cox, 2015). Since one of the extremist organisations' modus operandi is to claim responsibility for and exploit the results of an attack, non-attribution would be out of kilter with these organisations' operational (and perhaps strategic) goals. One exception to this would be hacktivist organisations. Hacktivist organisations make a point of claiming responsibility for their cyber exploits; however, they are careful to erase their digital footprint in the targeted systems so that digital forensics cannot be performed (Seebruck, 2015).

Cost is another barrier. While offensive cyber operations can be executed by an individual at relatively low cost, operations that are more complex will require greater resources and involve more than one operator. The procuring of equipment, encryption software, exploits, and personnel to manage the operation can all potentially generate an enormous overhead and draw unwanted attention (Goncharov, 2013; Greenberg, 2012; Fortinet, 2012; Fossi et al., 2008). Furthermore, if the objective of the cyber attack does not merit the cost, then the operation can implode. Cost, therefore, is assessed to be the reason why most offensive cyber operations

conducted by non-state actors today tend to be associated with achieving monetary gains (Goncharov, 2013; Greenberg, 2012; M86 Security Labs, 2010).

Sustainability (or lack thereof) can serve as a barrier to extremist organisations engaging in offensive cyber operations. Sustainability is what separates an ordinary hacker from an Advanced Persistent Threat (APT). Offensive cyber operations rarely take a few minutes to execute. Rather, they are time-consuming affairs that may or may not yield acceptable results. It takes months, sometimes years, to plan and execute a complex cyber operation with no guarantee of any return on investment. There are very few extremist organisations that can afford and maintain the commitment to see it through, with potentially no visible benefit, for an extremely narrowly focused objective (Seebruck, 2015; Finklea et al., 2015).

The literature clearly demonstrates the potential advantages and relative ease of engaging in offensive cyber operations for a motivated individual or extremist organisation. It also provides several substantial reasons that could deter extremist organisations from engaging in and incorporating offensive cyber operations into their attack portfolios; however, there are a few notable deficiencies in the literature. First, it only examines the extremist organisations' use of offensive cyber operations as a standalone cyber exploit. For example, it assesses disruption-focused cyber weapons and the non-attributive nature of the offensive cyber operations as potential deterrents. These assessments may absolutely be correct if one only considers cyber only operations. However, as soon as one moves to combined cyber and physical operations where cyber operations are designed to facilitate the physical operations of traditional kinetic terrorist attacks, disruption and non-attribution of the cyber domain may just be what an extremist organisation needs to successfully execute the kinetic attacks in the physical domain. Second, the literature currently does not take into consideration the wide-ranging variations between extremist organisations in a systematic manner. Since variances in organisational characteristics can contribute to organisational behaviour, a systematic understanding of organisational characteristics can contribute to an extremist organisation's higher likelihood of obtaining or developing offensive cyber capabilities as well as engaging in offensive cyber operations is necessary.

3. RESEARCH DESIGN AND METHODOLOGY

Since there are no preceding studies that systematically examine the human and organisational aspects of offensive cyber operations in the context of terrorism, a structured expert elicitation was conducted to identify potential explanatory variables against which to collect data in Phase II. The structured expert elicitation was designed to ascertain expert assessments on the relative importance of various organisational characteristics. The primary tool used for this structured expert elicitation was a survey, and the participants were all currently active members of the public sector, private sector, or academia working on issues relevant to cyber security.

The survey consisted of presenting the experts with a set of 22 independent variables, and asking them to rate each variable on a five-point ordinal scale. These variables were drawn from

the list of extremist organisational variables and profiles of existing extremist organisations developed by START[2] and maintained over the past decade. Table 1 provides the list of all 22 organisational factors presented to the experts. The variables were grouped into four distinct factors based on their characteristics: organisational, resource, sophistication, and prior activities.

We recruited two groups of experts to serve as potential participants – those with technical backgrounds in subjects such as computer science or computer engineering, and those with non-technical backgrounds including policy makers, policy analysts, and academics. Once the potential participants were identified, the survey with detailed instructions was sent to them by email. All participants received the same survey. The survey response rate was 18.67%.

The collected data was coded into a format where statistical analysis could be performed to identify the variables that the participants assessed as having the most probabilistic explanatory power for determining an extremist organisation's likelihood of choosing to engage in offensive cyber operations. Table 2 provides a full list of participant groupings used in the analyses of the survey results, and the findings from the analyses are discussed in the next section.

4. FINDINGS

A. Overview

The data collected revealed there are several points of convergence, as well as divergence in the participants' assessment of organisational characteristics that could be significant in forecasting whether an extremist organisation is more or less likely to incorporate offensive cyber operations into its attack portfolio. Overall, there was a general consensus among the experts that *level of Internet presence, access to human resources*, and *human resource available* (internally to the organisation) are the variables with the most probabilistic explanatory power. The analysis of the survey results (see Table 3) found that the *level of Internet presence* of an organisation was the most important variable, while the statistical analysis of the results (see Table 4) revealed *access to necessary human resources* as the most powerful explanatory variable. Although *access to necessary human resources* was not found to be rated as the most important variable, it was in the top five variables (see Table 3), demonstrating that a degree of congruence does exist between the survey and statistical analyses results. The remainder of this section discusses the results of the analyses in further detail, beginning with the overall survey results.

B. Overall analysis

1) Results of survey analyses

The survey analysis found that the *level of Internet presence* of an organisation was rated as the most important variable by the participants. Their reasoning, according to their responses to the open ended questions in the survey, was that even if the organisation did not currently does not

2 Established in 2005, the National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a research and education centre based at the University of Maryland and comprised of an international network of scholars committed to the scientific study of the causes and human consequences of terrorism in the United States and around the world. As a U.S. Department of Homeland Security Centre of Excellence, START supports the research efforts of leading social scientists at more than 50 academic and research institutions, each of whom is conducting original investigations into fundamental questions about terrorism.

have offensive cyber capabilities or had not engaged in offensive cyber operations, the fact that an organisation has a favourable disposition towards conducting portions of its operations in the cyber domain means it would be more comfortable with the idea of offensive cyber operations, and be more likely to consider incorporating offensive cyber operations into its attack portfolio, either as a standalone capability or as a part of a comprehensive cyber and physical attack package (Sin, et al., 2015). The participants also assessed that organisation's *leadership, access to human resources*, and *human resources available* (internal to the organisation) are top organisational characteristics (see Table 3).

Despite the fact that some consensus can be found in the participants' responses, there were some significant divergences in the ratings as well. For example, participants with technical backgrounds and those working in the public sector, rated *financial resources* available to the organisation as one of the top variables, while those with non-technical backgrounds and those who works in the private sector and academia included the organisation's *penchant for innovation* and *propensity for violence* in the list (see Table 3). *Access to necessary human resources* – the most significant variable in the statistical analyses – was assessed as one of the top five variables by four of the six participant groups. Figures 1 to 6 show the analyses of the participants' ratings of all variables. An interesting result shown in these figures is that the participants rated variables such as *ideology, organisational structure, organisational size*, and *network connections and access* – all factors found to be extremely significant in determining organisational behaviour and lethality in terrorism literature (Asal, Ackerman, and Rethemeyer, 2012; Asal and Rethemeyer, 2008; Gill, et al., 2014) – to be less important factors in forecasting an extremist organisation's likelihood of engaging in offensive cyber operations.

2) Results of statistical analysis

Statistical analysis conducted on the survey data to determine which variables the participants rated as having the highest explanatory power, found *access to necessary human resources* to be most significant. *Propensity for violence* and *human resources available* were found to be the second and third most significant respectively (see Table 4). All three variables were also found to be significant in the survey analyses, and all of the variables found to be significant in the statistical analysis are included in the list of top five most significant variables ascertained through the survey analysis (see Table 3).

The combined results of the statistical and survey analyses indicate there is a general consensus among the experts that *access to necessary human resources; propensity for violence; human resources available; level of internet presence; leadership characteristics;* and *penchant for innovation* are the most significant characteristics with explanatory power for predicting an organisation's likelihood of engaging in offensive cyber operations in the future.

C. Group analyses

A series of survey analyses were performed on five distinct groups of participants (see Table 2 for a list of groupings) to obtain a more nuanced understanding of the survey responses. The analyses revealed some very interesting within- and between-group trends. In general, a comparison of results between technical and non-technical groups yielded a very different picture than a comparison of results across the public sector, private sector, and academic

groups. Different groups, independently of each other, also exhibited clear and distinct trends of thought. Examining all of the seemingly disparate results, we were able to extrapolate that *Internet presence, leadership,* and *penchant for innovation* were considered to have the most probabilistic explanatory power. A more detailed comparison is discussed below.

1) Technical – non-technical group analysis

Overall, the technical group exhibited a higher within-group consensus on the importance and non-importance of variables than the non-technical group. The technical group tended to place relatively higher importance on the variables belonging to the *prior activities* factor such as *prior terrorist activities* and *propensity for violence*. Furthermore, the group placed a high value on the usability of resources such as *access to human resources*. The group also tended to assess variables relevant to organisational, membership, and leadership characteristics as being important, but to a much lesser degree than the organisation's prior activities and resources available. By contrast, the non-technical group placed the highest importance on the variables belonging to the *sophistication* factor, favouring the technical aspects of the organisation's characteristics, while assessing the variables belonging to other factors as less important or not important at all.

The analyses clearly showed a divergence in the perspectives on *organisational* factor between the two groups. Overall, the non-technical group assessed *organisational size* and *membership cognitive distortion* as not being important at all, while assessing *membership composition* as being almost neutral. The technical group, by contrast, assessed these factors as being more important compared to the non-technical group. Additionally, the technical group showed a tendency to place greater importance on leadership related variables than the non-technical group.

The technical group showed a strong consensus on variables belonging to *resource factors*. Of note, the two groups were shown to have an opposing view on *network access*, with the technical group assessing it not to be important and the non-technical group assessing it otherwise, albeit at a minimum importance. On other variables belonging to this factor, however, the two groups showed general agreement, with the technical group placing a much higher importance on them than the non-technical group.

The two groups showed a consensus in assessment for the variables belonging to the *sophistication* factor. Although there were some differences in the degree of importance placed on the variables between the two groups, they generally viewed all variables belonging to this factor as not being important with the exception of *Internet presence*, which was assessed as highly important by both groups.

2) Public sector – private sector – academic group analysis

Analyses of the public sector, private sector, and academic groups revealed that the public sector group tended to give high marks to resource and technical variables, while giving relatively lower marks to organisational, organisational composition, and leadership variables. Although the group assessed *Internet presence* and human and financial resources to be of high importance, it did not assess *network access* as important. The analysis of the public sector

group revealed that it perceived the decision of an extremist organisation to engage in offensive cyber operations is primarily a function of human, materiel, and financial resource availability.

The private sector group viewed *penchant for innovation* and *network access* to be more important than *Internet presence*, while assessing human and financial resource variables as relatively unimportant, a distinct divergence from the public sector group. The private sector group was the only group to assess *ideology* as being important among all the groups. The group also acknowledged the importance of the leadership variables, but assessed the relationship between variables relevant to organisational structure, size, and membership and the extremist organisation's likelihood to engage in offensive cyber operations as being quite low. The analysis of the private sector group revealed that this group perceived the decision of an extremist organisation to engage in offensive cyber operations as primarily a function of innovative ideas and having access to a network that could provide a support infrastructure.

The academic group, departing from the other two groups, placed low importance on the variables related to technical, historical, human resources, financial, and network aspects of the organisational characteristics. Compared to the other groups, it placed the lowest value on the *ideology* of the organisation and the highest on the *leadership* characteristics. The group also assessed *organisational cohesion* and *member composition* as being important, while *organisational structure* and *organisational size* were assessed as not. The results revealed that the academic group perceived leadership characteristics and the relationship between the leaders as key factors that could predict which extremist organisations was mostly likely to engage in offensive cyber operations.

Some interesting divergences were observed in the groups' assessments of the *organisational* factor variables. The private sector group was the only group that assessed *ideology* as being important, and the other two assessed it as strongly negative (unimportant), and the academic group was the only one to assess *membership composition* as being important. Additionally, the public group assessed *leadership* as not being very important while the other two groups assessed it as being important. The academic group in particular assessed *leadership* to be extremely important. In fact, the academic group was the only group that assessed all leadership related variables (with the exception of *leadership cognitive distortion*) as being very important in predicting an extremist organisation's likelihood of engaging in offensive cyber operations.

Consensus was apparent amongst the three groups on the importance of *organisational structure* and *organisational size* as not being very important, with the private sector group assessing them most negatively (unimportant) compared to the other two groups. The consensus amongst the groups diverged once again in their assessment of *organisational cohesion* with both public sector and academic groups assessing it to be important and the private sector group assessing it to be unimportant.

5. CONCLUSION

As the first phase to understanding why extremist organisations are not incorporating offensive cyber operations into their attack portfolios, this research sought to identify potential explanatory variables that can be incorporated into the development of a violent extremist organisation dataset, which includes cyber relevant variables. Once developed, the dataset will be used to empirically determine the organisational characteristics that make violent extremist organisations more likely to engage in offensive cyber operations. The results of this determination can then be used to explore further why they do not appear to be engaging in offensive cyber operations as much as they theoretically could.

In this phase of the research, a structured expert elicitation was conducted through a survey where the participants assessed the importance of 22 variables. The results of the survey and the statistical analyses found the participants assessed organisations' *level of Internet presence, access to human resources*, and *human resources available* as the variables most likely to predict the likelihood of a violent extremist organisation's decision to incorporate offensive cyber operations into its portfolio.

This research was also able to identify some important points of consensus and divergence that exist between the various expert groups. The consensus and divergence in assessed importance of variables were most significant along the participants' background and occupation. Analysis of each group showed the participants tended to have internal consistency within their assigned groups, but the groups showed clear between-group divergence. Second, the group divergences based on participant backgrounds were much weaker than the divergences observed among occupation-based groups. The degree of variance was much higher among the public sector, private sector, and academic groups than between the technical and non-technical groups. Finally, each group had a varying degree of internal group consistency. Between the technical and non-technical groups, the technical group exhibited a much higher internal group consistency than the non-technical group. Among the public sector, private sector, and academic groups, the public sector group presented the highest degree of internal group consistency, followed by the private sector group. The academic group exhibited the least internal group consistency. These results not only illuminate the impact that occupation has on one's world view in terms of perspectives and the degree of conformity, but they also expose a lack of clear understanding among the groups about each other's perspectives.

Another interesting trend observed during this research was the similarity in the results between the technical and the public sector groups. While some differences did exist between the two groups, they shared similar assessments of variables, both in direction (important or not important) and magnitude. Given that the public sector group was divided almost equally between technical and non-technical participants (53% technical and 47% non-technical), this trend suggests that: 1) unlike the results of the overall technical – non-technical comparisons, a much higher degree of consensus exists between the technical and non-technical groups within the public sector; and 2) the non-technical experts and practitioners in the public sector appear to have responded to the survey closer to their technical counterparts than the non-technical

participants in the other two sectors. While the current research cannot ascertain the exact cause of these differences, it could be that non-technical experts and practitioners perhaps have more routine exposure to technical information and experts during the course of their work. This is only speculation, however, and is a topic worth examining in future research.

A. Implications

Although this research is only the first phase of a three-phase research endeavour, the results have yielded several issues that require some consideration. First, the research confirmed that there is no systematic research being conducted today to determine why some violent extremist organisations decide to engage in offensive cyber operations, while others do not. Neither does it explain why few violent extremist organisations engage in offensive cyber operations despite the purported ease of acquiring the tools necessary to carry out such an operation. The research confirmed our impression that there is an apparent lack of standardised indicators that can be used to identify which violent extremist organisations are more likely to engage in offensive cyber operations. They also indicate there is a clear divide in focus and opinion and no evidence of robust communication between the various disciplines and sectors involved in cyber security. Finally, the results suggest that there may be a higher level of technical/non-technical expert/practitioner consensus than in other sectors examined, and follow-on research examining the convergences and divergences among experts and practitioners in different sectors is warranted.

These implications highlight the pressing need for the experts and practitioners of cyber security of various backgrounds and occupational areas to bridge the fundamental divides that exist among them through communication and education. They also call attention to a need for a broader cyber security research agenda that is multilateral, multidiscipline, and multimethod, and is designed to incorporate stakeholders from all sectors of society to address the challenges of the future cyber threat-scape.

B. Further research

Narrowing the focus back to the current research, we have developed the violent extremist organisation dataset that includes cyber-relevant variables by appending the cyber variables to the Big, Allied and Dangerous (BAAD) dataset (Asal, Rethemeyer, and Anderson, 2011), creating an extremist organisation cyber attack dataset. We are currently engaged in data collection following which, a series of follow-on research projects can be conducted to further explicate extremist organisations' likelihood of engaging in offensive cyber operations. Results from this research will allow an empirically based and more nuanced understanding of the relationships between terrorism, cyber, and extremist organisational behaviour.

ACKNOWLEDGMENTS

We would like to thank all of the subject matter experts who participated in the survey for this phase of the research. The team would also like to thank Dr Gary Ackerman, Director of Unconventional Weapons & Technology Division of START, University of Maryland, and Dr H. Sophia Sin, Research Associate of the Centre for Policy Research, State University of New York at Albany, for their support and encouragement throughout the course of this research.

REFERENCES

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. National Security Research Division, RAND Corporation, Santa Monica, CA: RAND Corporation, 85.

Archer, Emrald M. 2014. 'Crossing the Rubicon: Understanding Cyber Terrorism in the European Context.' *The European Legacy* 19 (5): 606-621.

Asal, Victor, Gary Ackerman, and R. Karl Rethemeyer. 2012. 'Connections Can Be Toxic: Terrorist Organisational Factors and the Pursuit of CBRN Weapons.' *Studies in Terrorism and Conflict* 35: 229-254.

Asal, Victor, and R. Karl Rethemeyer. 2008. 'The Nature of the Beast: Terrorist Organisational Characteristics and Organisational Lethality.' *Journal of Politics* 70 (2): 437-449.

Asal, Victor, R. Karl Rethemeyer, and Ian Anderson. 2013. 'Big Allied and Dangerous (BAAD) Database, 1998-2012'.

Bloom, Dan. 2015. 'ISIS Trying to Launch Deadly Cyber Attack on Airports, Hospitals, and National Grid, Warns George Osborne.' *The Mirror*. November 17. Accessed December 30, 2015. http://www.mirror.co.uk/news/uk-news/isis-trying-launch-deadly-cyber 6845517.

Cox, Christopher. 2015. 'Cyber Capabilities and Intent of Terrorist Forces.' *Information Security Journal* 24 (1-3): 31-38.

Finklea, Kristin, Michelle Christensen, Eric Fischer, Susan Lawrence, and Catherine Theohary. 2015. 'Cyber Intrusion into U.S. Office of Personnel Management: In Brief.' CRS Report No. R44111, Congressional Research Service.

Fortinet. 2012. 'Cybercriminals Today Mirror Legitimate Business Processes.' 2013 Cybercrime Report, Fortinet, Inc.

Fossi, Marc, Eric Johnson, Dean Turner, Trevor Mack, Joseph Blackbird, David McKinney, Mo King Low, Teo Adams, Marika Pauls Laucht, and Jesse Gough. 2008. 'Symantec Report on the Underground Economy July 07-Jun 08.' Symantec Corporation.

Gill, Paul, Jeongyoon Lee, R. Karl Rethemeyer, John Horgan, and Victor Asal. 2014. 'Lethal Connections: The Determinants of Network Connections in the Provisional Irish Republican Army 1970 – 1998.' *International Interactions: Empirical and Theoretical Research in International Relations* 40 (1): 52-78.

Goncharov, Max. 2013. *Russian Underground* 101. Trend Micro Incorporated.

Greenberg, Andy. 2012. *Shopping for Zero Days: A Price List for Hackers' Secret Software Exploits*. March 23. Accessed December 28, 2015. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

Kenney, Michael. 2015. 'Cyber Terrorism in a Post-Stuxnet World.' Orbis 59 (1): 111-128.

M86 Security Labs. 2010. *Web Exploits: There's an App for That*. M86 Security.

NTT Group. 2015. *Exploit Kits: Development and Operation Lifecycles*. Global Threat Intelligence Report, NTT Innovation Institute, LLC.

Pagliery, Jose. 2015. 'ISIS is Attacking the U.S. Energy Grid (and Failing).' *CNN Money*. October 16. Accessed December 30, 2015. http://money.cnn.com/2015/10/15/technology/isis-energy-grid/.

Pawlak, Patryk, and Cecile Wendling. 2013. 'Trends in Cyberspace: Can Governments Keep Up?' *Environment Systems & Decisions* 33 (4): 536-543.

Perlroth, Nicole. 2015. 'Security Experts and Officials Diverge on ISIS as Hacking Threat.' *The New York Times*. December 24. Accessed December 29, 2015. http://www.nytimes.com/2015/12/25/technology/security-experts-and-officials-diverge-on-isis-as-hacking-threat.html?_r=0.

Peterson, Dale. 2013. 'Offensive Cyber Weapons: Construction, Development, and Employment.' *Journal of Strategic Studies* 36 (1): 120-124.

Ponangi, Preethi Vinayak, Phani Kidambi, Dhananjai Rao, Narasimha Edala, Mary Fendley, Michael W. Haas, and S. Narayanan. 2012. 'On the Offense: Using Cyber Weapons to Influence Cognitive Behaviour.' *International Journal of Cyber Society & Education* 5 (2): 127-150.

Seebruck, Ryan. 2015. 'A Typology of Hackers: Classifying Cyber Malfeasance Using a Weighted Arc Circumplex Model.' *The Journal of Digital Investigation* (14) 3: 36-45.

Sin, Steve S., Elvis Asiamah, Laura A. Blackerby, and Rhyner Washburn. 2015. *Survey Conducted for CyCon 2016 Research*. College Park, MD, November 1.

Weissman, Cale Guthrie. 2015. 'It's Becoming Easier and Easier to 'Rent a Hacker'.' *Business Insider*. May 12. Accessed December 29, 2015. http://www.businessinsider.com/the-hacker-for-hire-market-is-growing-2015-5.

Zhang, Meng, Niraj Jha, and Anand Raghunathan. 2014. 'A Defense Framework Against Malware and Vulnerability Exploits.' *International Journal of Information Security* 13 (5): 439-452.

TABLES AND FIGURES

FIGURE 1: RATING OF ORGANISATIONAL FACTORS FOR FORECASTING LIKELIHOOD OF OFFENSIVE CYBER OPERATIONS (ALL PARTICIPANTS)

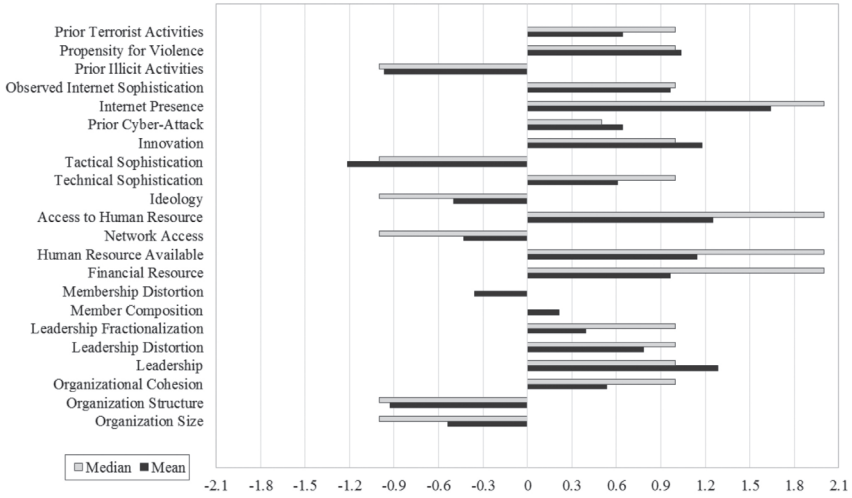

FIGURE 2: RATING OF ORGANISATIONAL FACTORS FOR FORECASTING LIKELIHOOD OF OFFENSIVE CYBER OPERATIONS (TECHNICAL PARTICIPANTS)

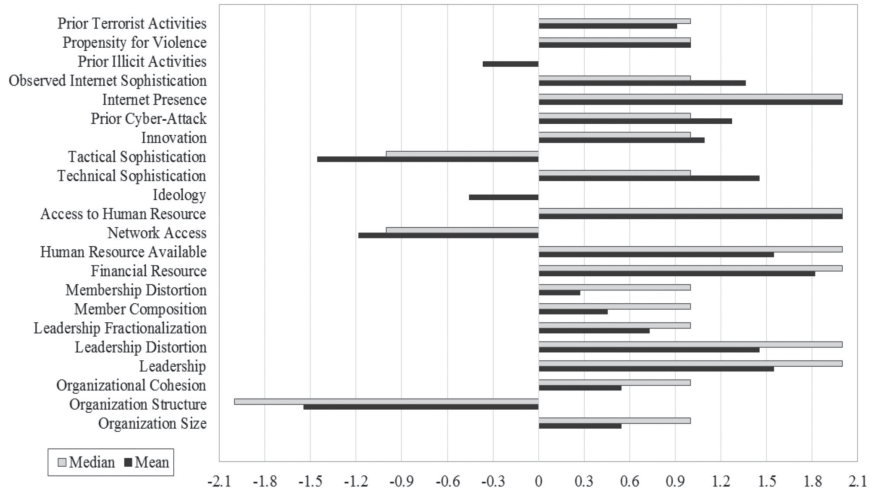

FIGURE 3: RATING OF ORGANISATIONAL FACTORS FOR FORECASTING LIKELIHOOD OF OFFENSIVE CYBER OPERATIONS (NON-TECHNICAL PARTICIPANTS)

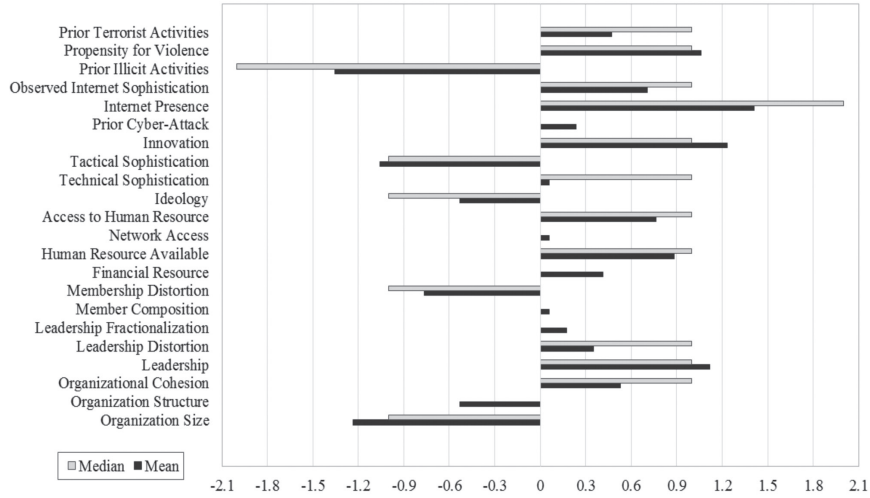

FIGURE 4: RATING OF ORGANISATIONAL FACTORS FOR FORECASTING LIKELIHOOD OF OFFENSIVE CYBER OPERATIONS (PUBLIC SECTOR PARTICIPANTS)

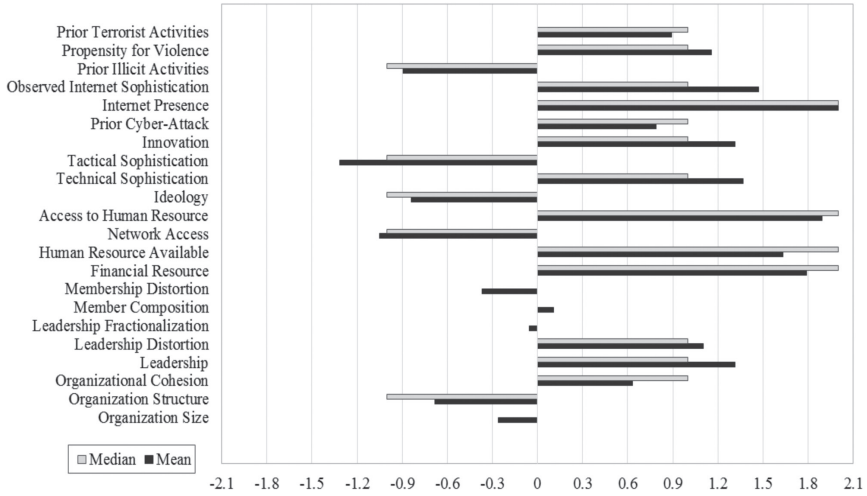

FIGURE 5: RATING OF ORGANISATIONAL FACTORS FOR FORECASTING LIKELIHOOD OF OFFENSIVE CYBER OPERATIONS (PRIVATE SECTOR PARTICIPANTS)

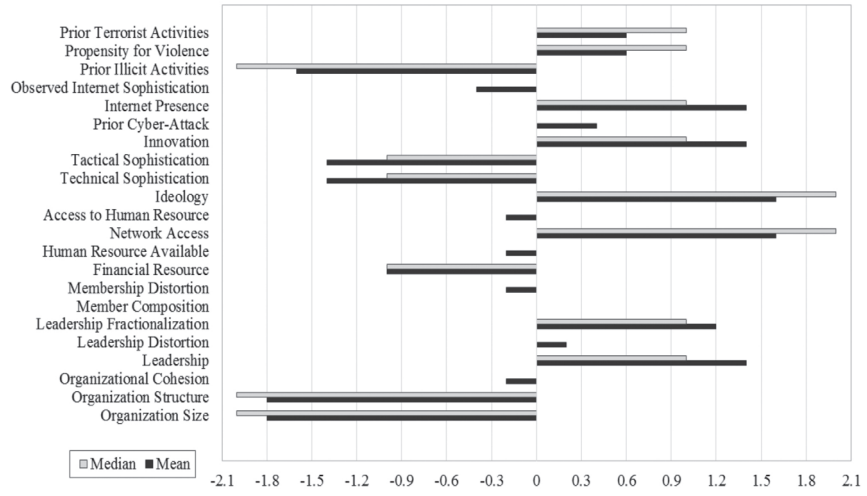

FIGURE 6: RATING OF ORGANISATIONAL FACTORS FOR FORECASTING LIKELIHOOD OF OFFENSIVE CYBER OPERATIONS (ACADEMIC PARTICIPANTS)

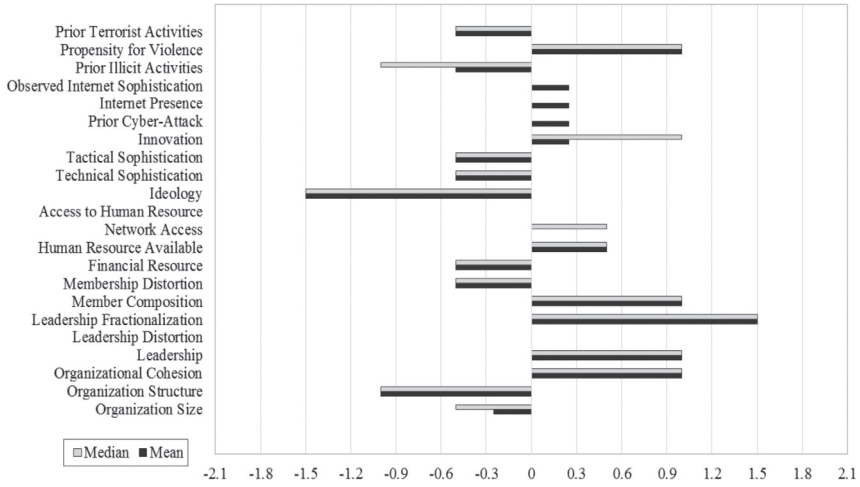

TABLE 1: ORGANISATIONAL CHARACTERISTICS INCLUDED IN THE SURVEY

Organisational Factors	Resource Factors	Sophistication Factors	Prior Activities Factors
Organisation Size	Financial Resources Available	Technical Sophistication	Prior History of Illicit Activities
Organisational Structure	Human Resources Available (Internal)	Tactical Sophistication	Propensity for (Prior History of) Violence
Organisational Cohesiveness	Network Connections & Access	Penchant for Innovation	Prior History of Cyber attack
Ideology	Access to Necessary Human Resources	Level of Internet Presence	Prior History of Terrorist Activities
Leadership		Observed Internet Sophistication	
Leadership Cognitive Distortion			
Leadership Fractionalisation			
Membership Composition			
Membership Cognitive Distortion			

TABLE 2: SURVEY PARTICIPANT GROUPINGS

Grouping 1	All Participants		
Grouping 2	Technical Participants	Non-Technical Participants	
Grouping 3	Public Sector Participants	Private Sector Participants	Academic Participants

TABLE 3: TOP FIVE ORGANISATIONAL CHARACTERISTICS RATING BY PARTICIPANT GROUPS (DESCRIPTIVE STATISTICS)

	Participants					
Rating	**All**	**Technical**	**Non-Technical**	**Public Sector**	**Private Sector**	**Academic**
1	Level of Internet Presence	Level of Internet Presence* Access to Human Resources*	Level of Internet Presence	Level of Internet Presence	Network Access* Ideology*	Leadership Fractionalisation
2	Leadership		Penchant for Innovation	Access to Human Resources		Leadership@ Organisational Cohesion@ Member Composition@ Propensity for Violence@
3	Access to Human Resources	Financial Resources	Leadership	Financial Resources	Level of Internet Presence# Penchant for Innovation# Leadership#	
4	Penchant for Innovation	Leadership^ Human Resources Available^	Propensity for Violence	Observed Internet Sophistication		
5	Human Resources Internally Available		Human Resources Available	Technical Sophistication		

* Tied for First
@ Tied for Second
\# Tied for Third
^ Tied for Fourth

TABLE 4: REGRESSION RESULTS (ALL PARTICIPANTS)

Dependent Variable: Organisation Engages in Offensive Cyber Operations

Independent Variable	Coefficient	Standard Error	T Score
Organisational Size	-.0116685	.083372	-0.14
Organisational Structure	.0254537	.0570688	0.45
Organisational Cohesion	.1014259	.0681252	1.49
Leadership	.0019509	.0570208	0.03
Leadership Cognitive Distortion	-.0052943	.0262764	-0.20
Leadership Fractionalisation	.0246953	.0506852	0.49
Membership Composition	-.00218	.0384258	-0.06
Membership Cognitive Distortion	.0183884	.0349441	0.53
Financial Resources Available	-.0743241	.0565408	-1.31
Human Resources Available (Internal)	.0487971	.0175308	2.78**
Network Connections and Access	.0532817	.0328357	1.62
Access to Necessary Human Resources	.0746465	.0237544	3.14**
Ideology	.025081	.0423652	0.59
Technical Sophistication	.0157153	.0607535	0.26
Tactical Sophistication	-.0097967	.0417712	-0.23
Penchant for Innovation	.0050692	.0239459	0.21
Prior History of Cyber attack	-.0040141	.0418024	-0.10
Level of Internet Presence	-.0069046	.0513136	-0.13
Level of Internet Sophistication	.0064245	.0448341	0.14
Prior History of Illicit Activities	.0306632	.0347698	0.88
Propensity for (Prior History of) Violence	.0630513	.015214	4.14***
Prior History of Terrorist Activities	.0383541	.0343559	1.12
Constant	.8387801	.2256389	3.72***

R-squared: 0.9977
All significance tests are two-tailed: *p<0.05; **p<0.01' ***p<0.001
Robust Standard Error used for Analysis