Integrating Human Behavior into the Development of Future Cyberterrorism Scenarios

Max Kilger
Department of Information Technology and Cyber Security
University of Texas at San Antonio
San Antonio, USA
Max.Kilger@utsa.edu

***Abstract*—The development of future cyberterrorism scenarios is a key component in building a more comprehensive understanding of cyberthreats that are likely to emerge in the near- to mid-term future. While developing concepts of likely new, emerging digital technologies is an important part of this process, this article suggests that understanding the psychological and social forces involved in cyberterrorism is also a key component in the analysis and that the synergy of these two dimensions may produce more accurate and detailed future cyberthreat scenarios than either analytical element alone.**

Keywords-cyberterrorism; scenario; social; psychological; motivation

I. INTRODUCTION

The development of a comprehensive understanding of the nature and evolution of cyberterrorism is one of the more important near-term tasks facing research scientists, policy makers and governments today. The speed at which digital and other cyber-related technologies are evolving combined with the inevitable engineering and marketplace forces encouraging the interconnection of devices, networks and systems is quickly outstripping our willingness and ability to foresee vulnerabilities and windows of opportunity that can be exploited by individuals, groups, organizations or nation states with terrorism related goals and objectives.

The vast majority of efforts to provide for the security of these devices and systems often are defensive and post hoc in nature, reacting to already present threats and newly discovered vulnerabilities. One of the key issues is that the rate at which these vulnerabilities and threats are uncovered and resolved by industry and governmental agencies is very likely smaller in magnitude than the rate of vulnerabilities being generated by new devices and technologies and the development of new threats by malicious actors. While the efforts being made to develop devices, networks and systems that are more secure and less vulnerable to attack or compromise are alleviating some of these threats, much of the danger still remains. Without a paradigm change in this limited defensive strategy, this gap in the aforementioned rates is likely to widen and the threat that it represents will become more serious in the near- to mid-term future.

One of the methods which holds some promise to provide relief from this situation is the development of future threat scenarios, particularly in the arena of cyberterrorism. The development of future threat scenarios accomplishes several key objectives. First, developing scenarios can sometimes illuminate vulnerabilities that are present in the present time frame by highlighting potential threats that may exist when current technologies are combined in unique ways. It may also be the case that developing future scenarios may highlight potential windows of opportunity for terrorist action for digital technologies that have not yet emerged or deployed in critical infrastructures or even in the consumer marketplace. This may provide organizations developing these technologies the opportunity to mitigate these vulnerabilities in the devices and systems they are developing. The creation of future threat scenarios may also provide policy makers with the opportunity to create policies and regulations that help thwart these new threat vectors that may appear in emerging technologies. The usefulness of developing future threat scenarios in reducing the exposure to cyberterrorism threats likely extends far beyond the simple examples mentioned.

One of the key suggestions of this paper is the idea that the value of future threat scenarios is likely to be significantly enhanced if psychological and social factors are incorporated into their development. Often it is the case that scenario-based threats to digital devices, systems and networks focus almost entirely upon the actual technical details of the vulnerabilities and the exploits that are developed to take advantage of them. Scant attention is often paid to cultural, social and psychological components that make up the human element of the threat. It is often forgotten that cyberthreats do not arise sui generis from the environment but in fact there is a human or group of humans somewhere in the causal chain.

This article provides some brief background on the relationship between human action and cyberterrorism on an individual, group and macro-level and then proceeds to outline how these human-based processes may interact with emerging digital technology to form scenarios of future cyberterror threats.

978-1-4673-6590-1/15 $31.00 © 2015 IEEE
DOI 10.1109/ARES.2015.105

II. INTEGRATING PSYCHOLOGICAL FACTORS

There has been a substantial effort in recent years to develop a better understanding of the psychology and mindset of terrorism – the reader may refer to several classic texts on the matter such as Post [1] or Hoffman [2] to obtain a more comprehensive grasp of the psychological motivations of classic terrorists and terrorist acts. However, it is much less clear how much of this body of work accurately applies to the motivations and mindset of the cyberterrorist. There is a significant paucity of theory and examination of the psychology of the cyberterrorist. Rogers [3] has written about the psychology of the cyberterrorist but the chapter focuses much of its attention on environmental factors that facilitate cyberterrorism and much less on the psychological processes involved. Others like Gross, Canetti and Waismel-Manor have examined and compared the potential psychological effects of cyberterrorism versus traditional terrorism on the population [4]. On a more general theme, Kilger [5] examines the psychology of cyberviolence and finds that there are six basic motivations: Money, Ego, Entrance to social group, Cause, Entertainment and Status (MEECES). It is likely that some of these motivations may also apply to some aspects of cyberterrorism.

Another early approach to better understanding cybercrime and the hacking community was the Hacker Profiling Project sponsored by the United Nations Interregional Crime and Justice Research Institute (UNICRI). Phase one of this project started in 2004 and lasted until 2010. Among the objectives of this research initiative was the idea to produce a taxonomy of different types of hackers responsible for cybercrime as well as begin to construct representations of the organizational structure of cybercrime enterprises. This taxonomy classified hackers by skill level, group or individual threat type, target type, basic demographics and level of threat. Phase two of this project according to Bosco [6] has continued this work, branching out more into motivations and behaviors of new hackers emerging on the scene as well as some additional focus on cyberterrorism and malware analyses.

More specifically focused on the psychology and root causes of cyberterrorism are two additional sources. Kilger [7] in a similar fashion to Rogers outlines some of the environmental factors that may likely encourage cyberterrorism. These factors include low probability of apprehension, higher than average probability of success, low cost of developing and deploying the attacks and the potential for orders of magnitude increase in potential damage over more traditional forms of terrorism. However, Kilger then suggests that these factors from a social psychological perspective non-trivially affect the traditional balance of power between the individual and the nation state. In fact, he suggests that the factors alter the psychological balance of power that has traditionally existed between the individual and the state such that for the first time in history an individual can effectively attack a nation-state.

In one of the few studies of its kind, Holt, Kilger Chiang and Yang [8] conducted a trans-national study of some of the potential factors involved in the intent to commit a specific cyberterrorist act on either on a foreign country or upon their own homeland. The study design was a 2 x 2 configuration of type of terrorist action (cyber versus physical) by target of attack (domestic versus foreign) as shown in Table 1. The dependent variable in this case was the severity of the cyberattack. Three different statistical models were applied to cyberattack intentions: a model with cybercrime related predictors, a model with political predictors and a third model that combined both types of predictors.

TABLE 1. EXPERIMENTAL DESIGN

	Target of Attack	
Type of Attack	Foreign Country	Homeland
Cyber	Cell 1	Cell 2
Physical	Cell 4	Cell 3

An initial examination of bivariate correlations suggested that spending more time online was positively correlated with willingness to engage in cyberattacks. Engaging in past acts of software piracy were also positively correlated with willingness to engage in cyberattack acts in general.

When the analysis compared the three types of multivariate models against specific types of cyberattack across the four cells of the study design however, a much more complex and varied set of patterns began to emerge. Surprisingly, measures of nationalism and patriotism as outlined in scales by Kosterman and Fesbach [9] had little effect across most of the models. The level of ingroup/ outgroup antagonism as posed by Sidanius and Pratto [10] was positively related to the probability of committing a cyberterror act for some types of acts but this effect often disappeared when these variables were introduced in the combined cybercrime-political model. When applying the combined model to the probability of compromising a military server, those who feel that law enforcement does not realize when cybercrime occurs, outgroup antagonism and physical protest actions are associated with an increased probability of attacking a military server. It is quite evident from the results of the statistical models in this study that the relationship between different types of predictive variables and the probability of intending to commit a specific type of cyberterror act is complex and requires significantly more study.

Finally, one of the key findings from this study was the strong correlation between the intentions to commit an act of cyberterrorism versus intention to commit a traditional physical act of terrorism. This suggests that there are some yet unknown mechanisms that help determine whether the individual eventually pursues a cyber-based mechanism of terror or a more traditional physical one. It also suggests that there may also be some propensity to combine both cyber and physical terror actions, an issue that has concerned counterterrorism researchers and officials for some time.

III. MESO- AND MACRO-LEVEL SOCIAL DYNAMICS AND FORCES

Individual level forces are not the only phenomenon that should be considered being integrated into the development of future cyberattack scenarios. Cyberterrorist acts may in fact be the product of a group of actors rather than a "lone wolf" individual. Gaining a better understanding of the networks that cyberterrorists form may likely be useful in understanding communication patterns, leadership structures and inter-group alliances that may help portend future threats that might emerge from these groups.

Studies of networks of traditional terrorist groups - see Perliger and Pedahzur [11] for an example – can be useful in linking potential group members as well as groups and determining characteristics of group members such as relative power in the group. While there has been little research in the open source literature about the structure of cyberterrorist networks specifically, there are likely lessons to be learned from examining networks of malicious online actors regardless of their ultimate act. For example, Holt, Strumsky, Smirnova and Kilger [12] analyze the ties between malicious online actors who are members of a number of Russian hacking gangs. This research revealed that there were some individuals that belonged to more than one hacking group, which suggests that these "connector" type individuals may be a key part of information exchange and coordination among the different Russian hacking groups. They also found that individuals within a network who posed a higher risk threat in terms of expertise in general were also more popular in terms of the number of connections to them. It should be noted that, although not noted in the article, there were also some high threat individuals who were located on the periphery of the network and had very few within-group or outside-group connections to other individuals. These individuals may be actively employing operational security measures to maintain low visibility within the cyber environment.

Another group phenomenon of interest is the emergence of malicious online hacking groups that either are pursuing objectives that appeal to nation states or have been shown to have non-trivial ties to nation states, often through the nation state's security apparatus. The number and the magnitude of the threat from these groups is growing – Crowdstrike [13] provides some recent analysis and examples of these types of groups. The actual level of involvement that these individuals or groups have with various nation state entities is also likely to vary from situation to situation. Healy [14] has developed a 10-point ordinal scale that describes the level of involvement of the hacking group with nation state entities, which may be useful both in the analysis of the attribution of cyberterrorist attacks as well as proportioning out the assignment of responsibility for specific cyberterror acts or events.

It is likely that these "loose couplings" between hacking groups and nation state entities are not only going to become more prevent but stronger ties between these types of parties are also likely to emerge. While it appears from the open source literature that most of these cooperative enterprises involve the exfiltration of key documents and data related to important intellectual property held by industry as well as documents related to defense and intelligence matters, there is the distinct opportunity for nation states to engage these groups in cyberterror acts. Utilizing third parties such as hacking groups to provide the necessary skill as well as to execute acts of cyberterror also puts some distance between these acts and the nation state, making it more difficult to assign attribution for the acts and provide justification for sanctions by the nation state victim.

One interesting possible development in evolution of the relationship between hacking groups and nation state security services is suggested by Kilger [15]. As the relationship between the hacking group and the nation state begins to mature, the hacking group undergoes a transformation on several dimensions. As their skills and membership grow, both the perception as well as the reality of the power that the group may wield begins to build. This power manifests itself in the enhanced ability to attack more and more well defended systems and networks. Additionally, often these groups engage in non-trivial levels of financial cybercrime which in turn allows them to accumulate more and more funds and financial instruments that can be used to purchase computing and network equipment, software and even pay its members for their contributions. As the relationship with the nation state entity continues to strengthen, there is the potential consequence that association with these nation state entities, in particular the security services, works to establish the legitimacy of the hacking organization. In effect the hacking organization evolves into an entity with inherent technical, financial and political currency. Eventually they may even be in a position to negotiate or even challenge some of the nation state entities that have become willing partners in their enterprise. The direction that these hacking organizations eventually take – whether to engage in major cyberterror acts, turn on their former nation state partners – perhaps with a "bit of help from another nation state" – or even end up evolving into a legitimate business organization is unclear and it is suggested that the better understanding we have of these social and organizational dynamics, the more likely we will be able to shape them to our advantage.

IV. THE SYNERGY OF EMERGING TECHNOLOGY AND HUMAN ACTION

We are going to have to assume that digital technology is going to evolve at the same or even faster pace than we have already experienced. At least for the moment, absent the emergence of a technological singularity that heralds the arrival of sentient machines, the synergy between evolving digital technology and the psychological and socio-political forces is going to a great extent determine the purposes that this new technology is applied to. Possessing a more comprehensive understanding of the relationship between individuals and digital technology is going to provide researchers and policymakers with an advantage in helping to guide that synergy into productive rather than destructive pathways.

Applying old paradigms to this new synergy is not likely to bear bountiful, nor precious, fruit. During the early years of the recognition of cyberterror and cyberwarfare, there was a knee-jerk reaction to pull out the lessons learned from the nearest strategic analog that analysts could think of – strategic nuclear weapons. It soon became clear, however, that while there were some analogues to be made between the two technologies, there were very significant differences that made cyberthreats a very unique strategic weapon of terror in and of itself as succinctly noted by Libicki [16] and Krepinevich [17].

In addition, there is a fair amount of uncertainty about the future nature and shape of digital technology. In the near-term there is already a significant amount of energy and discussion surrounding the "Internet of Things" (IoT) as private enterprise rushes to inject connectivity into a large number of commercially available consumer products and services. As more and more devices become smart devices and their command and control as well as data communications get heaped onto the public Internet, the threat surfaces for the average individual begin to mount. As this author as well as others such as Macauclay [17] have observed, this trend may eventually result in the individual having the potential to be "surrounded by hostile devices" in both their physical as well as virtual worlds. The ability for cyberterrorists to reach out to individuals on a massive scale and effect physical and/or virtual damage to these individuals is fast becoming a reality. Indeed, as more and more physical devices get connected to the Internet in the coming age of the IoT, the connections and synergies between the virtual and physical world are likely to increase the magnitude of seriousness of this threat. In addition, note that unlike traditional acts of terrorism where the victims and consequences of the terror act were often isolated to a specific geographic area, cyberterrorism has the ability to reach out and effectively target specific ethnic, racial, religious, political, social class, demographic or other boundaries that were previously often more difficult or almost impossible to do.

Additionally, as Internet connectivity reaches more and more devices we may begin to see more and more cyberterrrorism that involves physical rather than cyber consequences. As consumer-based objects such as vehicles for example become more connected, the results of cyberterrorism become more deadly. Imagine a cyberterrorist whose objective is to target vehicles within a 1 square km radius and command them to accelerate to top speed and disable any braking mechanisms. The chaos and carnage would be considerable.

Another potential future cyberterror tactic along similar lines would be something that could be called "cyberspearing". Taking inspiration from the current strategy by Western nations to attack the leadership of terrorist organizations using kinetic force, cyberterrorists may use this "spearphish" strategy to target specific individuals in the military, government or other organizations as specific cyberterror targets. The fear, disruption and actual damage that this strategy may cause could make cyberspearing a very attractive tactic for cyberterrorists. This particular tactic could also end up on the menu of the militaries or security services of various nation states. Nation states may decide to wage cyberspear campaigns against key political or military leaders in other nation states as an effective strategy to harass, impede and otherwise alter national policies through the targeting of national leaders. These campaigns would be difficult to attribute and could become difficult to deter or stop.

Cyberterrorists utilize the military concept of force multiplier in a unique way. They take virtual or physical assets that they do not own but rather their targets do and turn them to their advantage either as targets or as weapons. The traditional terrorist utilized this tactic in a much more localized way. The 9/11 attacks are a good example of traditional terrorists acquiring assets owned by their adversaries – in the form of commercial aircraft – and turning them into weapons. Cyberterror holds a much larger threat in that these same tactics could be used but on a much larger scale. Whether it's the virtual commandeering of a entire large airspace filled with commercial aircraft or a group of chemical plants in a large industrial city, the consequences and potential damage from this strategy could be significant.

One flavor of the idea of cyberterrorist use of force multiplier is particularly worrisome. Rather than having to plan, prepare and conduct a cyberattack on a large number of targets or weapons, cyberterrorists could push the envelope of the concept of force multiplier through the execution of a plan to target just one military unit containing smart military hardware for a particular nation state, especially at some sensitive geographic flashpoint and use it to attack another nation state. The tactic of generating a small, localized military conflict that then spreads between the two nation states is perhaps the ultimate use of force multiplier in a cyberterror scenario. The cyberterrorists end up utilizing a small amount of resources and effort that in the end have two or more nation states utilizing their own resources against each other.

Another future scenario links cyberterror vectors to our increased reliance upon sensors, machines and augmented realities to form our world realities. Our perception of the world is beginning to evolve into a domain where our sense of the world around us becomes more and more dependent upon digital technology and devices. As our culture inserts more and more technology in the perceptual chain between our human senses and the objects/actions that occur in the world, the opportunities and vulnerabilities to alter those perceptions increases dramatically. Analogous to a current day "man in the middle" attack, the more we allow technology to observe, measure and influence our perception of the world around us, the more susceptible we are to malicious alteration of our perceptions and world view. The very early markers that suggest this threat may eventually materialize or may be already here.

As we rely upon digital devices to observe, report on and control our physical environment, to monitor the safety and security of the foods in the marketplace, to control and report back on critical infrastructure statuses and as individuals utilize augmented reality in the form of digitally enhanced perceptions (e.g. GoogleGlass), we widen the gap between our natural, unaltered senses and the phenomenon that we are attempting to observe and control. This widening gap becomes a nutritive environment where malicious actors – in this case cyberterrorists – can gain a foothold and take advantage of a fertile operating environment.

So far in all of our discussions, there has been the implicit assumption that various forms of terrorist motivations executed in the cyber environment are prime inspirations and motivators behind cyberterrorist acts and events. It is a simplified expectation that all cyberterrorist acts in the past, present and future will be guided by terrorist motivations and justifications. That is, there is a tautological flavor to the reasoning that (cyber)terrorist acts are motivated by terrorist motivations.

However, I would argue that in this argument one is confusing the consequences of the event with the motivation itself that led to the event. This I would hypothesize is especially true in the cyber environment. A series of cyber actions that result in a cyber or physical world event or events that would likely be labeled terrorist in nature may not always come from terrorist or ideological origins. I would point to the previous discussion of the motivations for malicious online acts as especially useful in this case. That is, the most straightforward argument for all of the acts of cyberterror discussed in this article would, utilizing the MEECES schema, be assigned to Cause.

It should be realized however, at the risk of repeating oneself, that the MEECES schema covers motivations for malicious online acts, for which cyberterrorist acts can be classified as an instance. Therefore, while it has not likely been discussed seriously before, cyberterrorist acts may also emerge as a result of other motivations in the theoretical schema – Money, Ego, Entrance to social group and Status. This is why it is important to approach important areas of research such as cyberterrorism from a theoretical perspective and also – echoing the thesis of this article – to include social and psychological aspects to the analysis of cyberterrorism. It is entirely feasible that an act or set of actions that would normally be labeled classical cyberterrorism may be motivated by money for instance. Gaining entrance to a traditional or cyber-based terrorism group by an individual or individuals might involve the execution of a cyberattack on some specific critical infrastructure elements in order to gain acceptance into the (cyber)terrorist organization or group. There is some non-trivial, non-zero probability that in the near- to mid-term future there will occur cyberterrorist acts that will be the result not of traditional terrorist motivations (e.g. Cause) but the result of one or more of the other theoretical motivations for malicious online actors.

The idea that cyberterror acts may be the result of something other than straightforward, traditional terrorist motivations including the usual political or ethnic goals means that the scope of individuals who may consider committing a cyberterror act has widened considerably. That is, as digital technology continues to advance and the relationship between people and digital technology evolves, the ecological niches where technological vulnerabilities coexist with individuals who have motivations to take advantage of those vulnerabilities may likely increase both in number and size. Failure to take into account non-traditional motivations for terrorist attacks - particularly in the arena of cyberterror - may leave individuals, organizations and nation states open to be blind-sided by cyberattacks in the near- to mid-term future.

Coalitions and communities are another social phenomenon of interest to researchers involved in better understanding terrorism behaviors. As was previously discussed, terrorist and malicious online actors often belong to small to moderate-sized social networks. Individuals often communicate and interact not only with other individuals within their own group but also across groups as well. Evidence for strong coalitions and cooperation among traditional terrorist groups is not prolific but where it exists Schreier [19] suggests that it takes two forms: hard links and soft links. Hard links consist in part of sharing financial resources, intelligence, safe havens and skilled personnel. Soft links that form cooperative actions among terrorists include opportunities, responsibility for a terrorist act where one organization may agree to take the public responsibility for a terrorist action of another and shared ideological viewpoints where one organization may publically support another organization's actions.

The relatively immature status of cyberterrorism groups may mean that cooperation or coalitions among these groups may be limited. However, there is evidence of cooperation among some malicious online actors that may take various forms such as exchanging various malware exploits that are then adapted and modified for further use or the trading of various stolen digital and financial resources such as compromised servers and passwords, stolen financial credentials, bitcoins and other difficult to trace financial instruments as well as other objects such as card skimmers. If one accepts the idea that cyberterrorists are an instance of malicious online actors, then it is possible once a more critical mass of cyberterrorists emerges these kinds of cooperation may also surface in the hard and soft link forms that Schreier has illuminated.

The final discussion revolves around the idea of a cyberterrorist community. Communities emerge and develop among individuals and groups who share a common set of norms and values. Digital communications are an ideal way in which to facilitate the formation of virtual communities where members are often separated by large geographical distances. The actual factual status of whether or not there is a cyberterror community is likely not known and may not be known for some time. However, it is important to build this particular structural element into future cyberterror scenarios because of the threat potential such a community would have on both virtual and physical worlds.

One of the interesting differences between how a traditional terrorism community and a cyberterrorism community would function is the difference in the efficiency with which members of the community can exchange the basic materials of their terrorist actions. While the acquisition and transport of traditional terrorist materials such as firearms, ammunition, explosives and other basic materials is often problematic and entails a fair amount of risk on the part of traditional terrorists, this risk is significantly mitigated when basic materials for cyberterrorists such as exploit code, passwords, IP addresses to compromised servers and more can be easily and quickly transported digitally with relatively less risk than traditional terror materials and at much greater speed in addition. While care must be taken by cyberterrorists to obfuscate or otherwise hide these digital materials to avoid detection by law enforcement and intelligence agencies, it would seem likely that at least for the moment this is an important advantage for cyberterrorists.

The same argument holds for the actual execution of the terrorist attack. The traditional attack involves again moving the material to the proximate geographical location of the target (with perhaps the exception of weapons such as longer range intermediate or ballistic missiles) and engaging in procedures to deploy the materials and execute the attack. Cyberterrorists often face similar difficulties in gaining virtual access to the target, however they may likely suffer less exposure or risk of discovery or apprehension utilizing these materials in executing the actual attack than would be the case for traditional terrorists.

These kinds of advantages not only reduce the risk to the cyberterrorist but they are also likely to encourage cooperation and specialization among different cyberterrorist groups. The quick and efficient exchange of intelligence, information and basic materials involved in cyberterror may facilitate the formation of coalitions and eventually nurture a global embryonic cyberterrorist community.

Indeed, this kind of evolutionary pattern of cooperation, specialization and organizational structure can already be seen developing amongst malicious online actors in the area of cybercrime. Thomas et al [20] outline in detail the emergence of a cooperative cybercrime community of technical specialists as well as providers of unskilled labor and service/fulfillment providers in a long value chain that represents all of the steps in tracing the exchange of capital, real or imagined services and materials between a customer or victim, and the primary cybercrime business operator or malicious online actor.

A key question that must be posed is, will the evolution of cyberterrorism follow a similar organizational path? There are important similarities between these two populations. They both involve malicious online actors and as was previously suggested, motivations for malicious online acts – whether they be classified as cybercrime or cyberterrorism – may be shared between the two communities. Additionally, the cyber environment may facilitate the blurring of lines in terms of what is classified as a cybercrime and what is classified as cyberterrorism. This may increase the difficulties that policymakers face when deciding how to create new policies to combat this threat, assign responsibilities to government and law enforcement agencies and allocate resources to each type of online malicious act.

Another key point that Thomas et al make is that a more comprehensive, strategic approach must be taken to combat cybercrime. They suggest that the isolated strategy of protecting users and systems is “tantamount to a firefight” and that information security researchers should concentrate on gaining a better understanding of the overall structure of cybercrime, identify frailties in that structure and attack those structural weak points. This suggests that information security researchers need to develop a better understanding of the organizational and social structure of the cybercrime community.

One macro-level research study that maps out the social structure of a specific online community where there is at least a partial presence of online malicious actors comes from Kilger [15]. This study decomposes the social structure of the hacking community and does so from two different points in time - 1994 and 2003 utilizing a content analysis of the Jargon File. The Jargon File was a hackers dictionary of sorts compiled online over the years by hackers from early on in the history of the hacking community until the Jargon File's demise effectively after 2003. This file contained several thousand entries, each of which was a word or phrase whose meaning within the context of the hacking community was then explained. The content analysis of this document uncovered 18 dimensions within the social structure of the hacking community as can be seen in Fig. 1 below. Each bar pair represents the incidence of the class of entry for both 1994 and 2003 respectively. The assumption here is that the more important the dimension within the social structure of the hacking community, the larger the incidence for that dimension in the Jargon File.

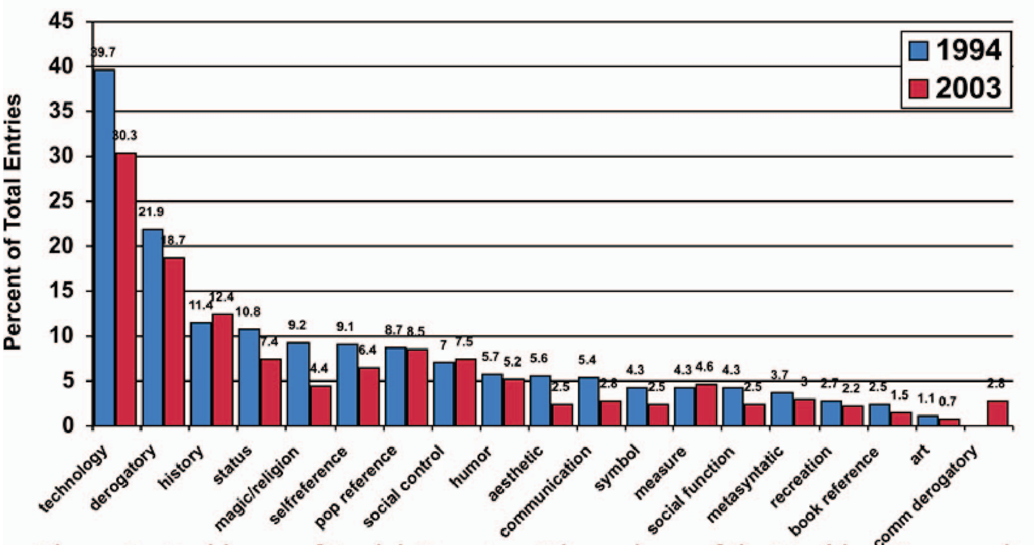

Figure 1. Incidence of Social Structure Dimensions of the Hacking Community

These dimensions included the roles of technology, the use of derogatory statements as social control processes, the presence and special meaning of magic as a religious element, social status processes and more. This type of analysis can assist information security researchers in identifying key social structure components of a population or community so that as Thomas et al suggest, they can be investigated to see whether or not frailties exist within those structures, whether there are obvious choke points in organizational processes or identify other weaknesses that can be exploited. This strategy should be workable regardless of whether the population is that of the hacking community or a more specific subpopulation such as a cyberterrorism subpopulation. In addition, the ability to measure these structural components over time may provide insight into how the social structure of the subpopulation may be evolving. This could prove useful in helping develop a better understanding of newly emerging cyberthreats.

V. SUMMARY

This article has covered two important points in examining the future of cyberterrorism. First is the idea that the development of future cyberterrorism scenarios should be considered a key component to understanding the shape and nature of cyberthreats in the near- to mid-term future. Developing these scenarios also provides researchers and policymakers with a tangible working model of these potential threats, provides an idea of the type and magnitude of consequences, allows them to devise possible defenses to these threats and gives policymakers insight into the resources that may be necessary to defend against them. Secondly, this discussion has emphasized the potential value of integrating psychological and social factors into the development of these scenarios in order to "color in" important details of these scenarios as well as estimate their potential likelihood of occurring.

REFERENCES

[1] J. Post, The Mind of the Terrorist: The Psychology of Terrorism from the IRA to al-Qaeda. New York: Palgrave Macmillian, 2007.

[2] B. Hoffman, Inside Terrorism. New York: Columbia University Press, 2006.

[3] M. Rogers, "The psychology of cyber-terrorism," in Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences, A. Silke, Ed. West Sussex: John Wiley & Sons, 2003, pp.77-92.

[4] M. Gross, D. Canetti, and I. Waismel-Manor, "Immune from cyber- fire? The psychological and physiological effects of cyberwar,"in Binary Bullets: The Ethics of Cyberwarfare, F. Alhoff, A. Henschke and B. Strawser, Eds. Oxford: Oxford University Press, forthcoming.

[5] M. Kilger, "The psychology of cyberviolence," in The Wiley- Blackwell Handbook on the Psychology of Violence, C. Cuevas and C. Rennison, Eds. New York: Wiley-Blackwell, forthcoming.

[6] F. Bosco, “The New Cybercriminals HPP: Hackers Profiling Project”, SECURE 2012, Warsaw, Poland, October 23, 2012.

[7] M. Kilger, “The emergence of the civilian cyber warrior,” in Cyber Infrastructure Protection, vol. 2, Carlyle, PA.: Strategic Studies Group, Army War College, 2013, pp. 53-82.

[8] T. Holt, M. Kilger, M. Chiang, and C. Yang., “Exploring the behavioral and attitudinal correlates of civilian cyberattacks,” in Social Networks, Terrorism and Counter-terrorism, M. Bouchard, Ed. Oxford: Routledge, forthcoming.

[9] R. Kosterman and C. Feshbach, “Towards a measure of patriotic and nationalistic attitudes,” Political Psychology, vol. 10, vol 2, 1989, pp. 257-274.

[10] JJ. Sidanius and F. Pratto, “The inevitability of oppression and the dynamics of social dominance,” in P. Sniderman and P. Tetlock Eds. Prejudice, Politics and the American Dilemma, Palo Alto, CA: Stanford University Press, 1993, pp. 173-211.

[11] A. Perliger and A. Pedahzur, “Social network analysis in the study of terrorism and political violence,” Political Science and Politics, vol. 44, issue 1, 2011, pp. 45-50.

[12] T. Holt, D. Strumsky, O. Smirnova and M. Kilger, “Examing the social networks of malware writers and hackers,” International Journal of Cyber Criminology, vol. 6, issue 1, pp. 891-903.

[13] Crowdstrike, Crowdstrike Global Intel Report, 2014.

[14] J. Healy, Beyond Attribution: Seeking National Responsibility for Cyber Attacks, Washington, D.C.: The Atlantic Council, 2012.

[15] M. Kilger, “Social dynamics and the future of technology-driven crime,” in T. Holt and B. Schell Eds. Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications, Hershey, PA: IGI-Global, 2010.

[16] M. Libicki, “The strategic use of ambiguity in cyberspace,” Military and Strategic Affairs, vol. 3, issue 3, 2011, pp. 3-10.

[17] A. Krepinevich, Cyber Warfare: A “Nuclear Option?”, Washington, D.C.: Center for Strategic and Budgetary Assessments, 2012.

[18 T. Macauclay, “.Social engineering in the Internet of Things,” March 2, 2015, retrieved from https://blogs.mcafee.com/ executive-perspectives/social-engineering-internet-things-iot on March 31, 2015.

[19] F. Schreier, “Combatting terrorism and its implications for intelligence,” in Terrorism and its Implications for the Security Security Sector, T. Winkler, A. Ebnother and M. Hansson Eds. Stockhom: Swedish National Defence College, 2005.

[20] K. Thomas, D. Huang, D. Wang, E. Bursztein, C. Grier, T. Holt, C. Kruegel, D. Mc Coy, S. Savage and G. Vigna, (2015) ‘Framing Dependencies Introduced by Underground Commoditization’, Workshop on the Economics of Information Security (WEIS). Delft University, The Netherlands, 22 June 2015.