Bahrun Naim's Hacking Manifesto: How a Historical Model of Cyber Threat Mischaracterization Helps us Diffuse a Dead Cyberterrorist Influencer

Tim Pappa
National Intelligence University, Bethesda, Maryland, USA

timothy.s.pappa@niu.odni.gov

Abstract: The late Bahrun Naim is generally considered one of the most recognizable names of historical Indonesian cyber terrorist actors, where he continues to be characterized as a "computer guru" and hacker who supported Indonesian extremist and Islamic State hacking. This paper is the first reexamination of Naim's lengthy e-book manifesto chapters on hacking, finding that most of the tutorial demonstrations on hacking tools readers might believe Naim performed were screen shots of other online content that Naim appeared to have plagiarized. This practitioner's paper suggests that Naim is a historical model of cyber threat mischaracterization, questioning who Naim was signaling with his hacking manifesto and why so many audiences including cyber threat analysts may have been influenced by reports on him. This paper evaluates Naim's *native* and *researched* technical knowledge based on his manifesto, suggesting the perception of Naim's native technical knowledge may have been embellished. This paper offers a conceptual interdisciplinary model for practitioners and researchers evaluating cyberterrorists' technical pedigrees and social environments. This model can also be applied to countering the range of cyber warfare including narrative warfare conducted by cyberterrorists, often revealing shortcomings in the mythos of cyberterrorists' influence and technical skills.

Keywords: Bahrun Naim, Cyberterrorism, Islamic State, Cyber behavioral analysis, Signaling theory

1. Introduction

The late Bahrun Naim is generally considered one of the most recognizable names of historical Indonesian terrorist actors, even outside of Southeast Asian counterterror watchers. Approximately twenty years ago, Naim was going to college and working at an internet café, but he had grown up attending Islamic boarding schools in Central Java, Indonesia, including schools prominently associated with some of the most significant Indonesian extremist leaders. These personalities joined what became Jemaah Islamiyah, an al Qaeda regional Southeast Asia affiliate responsible for the deadliest attacks throughout Indonesia in the early to mid-2000s.

Naim was also particularly close to many of these personalities who were close to Abu Bakar Ba'asyir, a Central Java extremist figure in Naim's hometown who had been exiled and later imprisoned related to an attack in the early 2000s. Ba'asyir was widely believed to be the spiritual head of Jemaah Islamiyah. Ba'asyir like Naim later pledged his allegiance to the Islamic State.

Naim was arrested in approximately 2010 and served about two-and-a-half years in Indonesian prison on charges related to illegally obtaining ammunition. Following his prison term, he affiliated with Islamic State and later appeared online in Syria, with his family. Before he left Indonesia, local authorities only considered him to be a "minor irritant".

Naim had a vocal role in facilitating or encouraging attack planning in Indonesia and the travel of Indonesian fighters to Syria, until he was killed in Syria in approximately 2018. Naim's role with Islamic State and his prior Indonesian extremist affiliations are questionable, considering he held no known leadership position and appeared to facilitate Indonesian travel to Syria largely on his own or with the help of his two wives. While there is some suggestion that Naim may have been trying to occupy a role with Islamic State as the leading Indonesian figure, much of this is speculation.

While there has been considerable attention to Naim's apparent role as one of the most "notorious" promoters of attacks throughout Southeast Asia, there has been limited to no attention to his writing on computer network operations and his background with computers. Naim has been historically characterized by much of the counterterrorism community as a "computer guru", who appeared to demonstrate his skills by operating multiple accounts on several platforms while being pursued in Indonesia and in Syria before his death in June 2018. Gunaratna (2018) has written extensively on Naim and Southeast Asian terrorism groups. Like Gunaratna, many observers refer to Naim's degree in informatics engineering and communication and his early use of cryptocurrency and encrypted messaging applications to facilitate attack planning as a demonstration of his technical knowledge.

This paper has limited perspective on who Naim's intended audience was and only general background on who some of Naim's peers were outside of these virtual communities. Naim was believed to have a "rolodex" of extremist contacts in Indonesia from his association with personalities affiliated with Hizbut Tahrir and Jamaah Ansharut Dauluh (JAD), which were much more regionally focused Indonesian collectives of extremists.

Naim appeared to be involved in some capacity with some of the other pockets of Indonesians in Syria as well, and these personalities also sent money and used social media. The audiences of cybercriminals or hacktivists of some sort in Indonesia that we might presume Naim wrote this e-book for were widely considered to be young but experienced in terms of carding and obfuscation. The more organized collectives or groups of Indonesian actors who conducted computer network attacks were characterized as "transitional", familiar with website defacements and Distributed Denial of Service (DDoS) attacks but unable to conduct scalable attacks against more desirable hardened networks. There were a handful of hacktivist groups supporting Islamic State in some form during this period and after Naim's death, with similar attack or tool capabilities. While this paper is questions who the target audiences were for Naim's manifesto, titled, "*Sebuah Perjalanan, Rahasia*" or "A Secret Journey", this paper is fundamentally exploring Naim's technical experience and capabilities. While there are understandable limitations in what we know about Naim's social experience at that time, identifying a contemporary cyberterrorist's technical flaws or other questionable technical behaviors could provide an opportunity to technically and informationally counter cyberterrorist cyber warfare.

2. Trying to Understand Naim's Signalling to his Audiences

Signaling theory is a foundational theory of communication, explaining how we evaluate how reliable what someone does is or how reliable what someone says is. Donath (2007) has characterized signaling theory as a framework for understanding and developing the communicative function of behavior. Generally, if the observable or presumed costs of signaling or displaying something appears to be more than the benefit of that communication, then the signal is probably reliable.

Donath and Liu (2006) wrote about people who appear to be or want to be 'fashionable' – for someone to be truly fashionable, there would be costs involved, such as time and attention to trends and to attending fashion events and costs associated with purchasing material and outfits. That reliability would probably be demonstrated in how responsive that person is materially or demonstrably to periodic shifts in fashion, which again would require costs. There would be more costs involved than benefits to someone falsely claiming and appearing to be 'fashionable', so that signal or display we see online is probably reliable. Here, Donath is highlighting the need to also consider the receiver of a signal or display.

Signaling theory also models highly contextual relationships among people that can explain why some signals or displays in that culture or group are reliable and others are not. Families with limited money in some cultures may still spend lavishly on a wedding as a "costly display" to demonstrate that they are wealthy enough to provide a wedding that meets norms, even if they will likely be more impoverished because of that wedding. While that example suggests there is significant cost involved, there is arguably more cultural benefit to that family and their son or daughter getting married to appear to be wealthy. What's most important here according to Donath is that the cost must be considered or occur in the appropriate domain, which in this case is a culture where lavish weddings are important "social capital" among families. If the same wedding occurred outside of this culture and among other people, the cost would be different and thus the signal would be different. Alvard (2023) in this context has characterized signaling theory when it involves people as fundamentally a theory of culture more than a theory of communication.

Donath referred to Zahavi (1977) who emphasized that costly signals are only understood in the domain or environment of that cost. Donath explained further that Zahavi referred to this foundational signaling context as the "handicap principle", where he suggested as an example that gazelles could afford to display what appear to be extravagant jumps even in the vicinity of predators because they must be fast enough to take those risks. But outside of that environment between predator and prey, whether gazelles are fast or not matters less in terms of cost. Donath has discussed this concept further, using biker gang tattoos as an example. While a gang member displaying his tattoo likely is a reliable signal of his gang affiliation, there would be significant costs for that presumed gang member if he was not actually a member of that biker gang and a real member of that gang discovered he was impersonating a gang member. We could imagine other possibilities as well, such as the display of a gang tattoo communicating to a rival gang member that if he chooses to harm that rival gang member, the victim's gang will likely respond – so the display or signal of the tattoo protects both bikers. Donath (2023) and Bliege et al. (2023) have both highlighted the importance of clear displays so that the sender and the receiver understand each other, often for the sake of each other's safety.

Lang et al. (2023) found in a study of commitment in groups that group members who demonstrated the most aggressive commitment to the group at first attracted more potential group members, including people who hoped for benefits without the same level of commitment. But those group members eventually left, as the committed group leader often influenced other group members to likewise demonstrate a similar level of commitment. The most committed groups with the most committed group leaders were found to be the most competitive and often the most successful in this study. Lang suggested that in situations that perhaps demanded "absolute commitment", observationally costly signals or displays did give those groups an advantage over other groups because of the shared commitment in the group. Even if members were forced to commit further, Lang wrote, generally their overall level of commitment was reinforced.

Donath emphasized that communicators want to be perceived *advantageously*, so they will use signals to communicate the cues they want the audience to see. Could Naim's release of this e-book represent a signal or display in his context of "absolute commitment", which might mean that once he released this manifesto that included diagrams and instructions for making bombs, then surely Western intelligence services would focus their efforts on Naim because he would appear to be a rising Indonesian leader in Syria, even if Islamic State leadership generally disregarded him in Syria? Did Naim begin his e-book with a preamble on the second page that appeared to be a disclaimer of sorts regarding his affiliation with the Islamic State, because he was not recognized by Islamic State leadership?

Naim wrote in this preamble that this e- State. However, later in Naim's introductory sections, he wrote that he is not a leader, and he has no desire to be a leader. Naim continued, asking rhetorically if the reader was "astonished" that he would write that he has no desire to be a leader. Naim wrote that he is already in the Islamic book are his "private" writings and that this work does not reflect the writings or works of the Islamic State. This paper questions what Naim was trying to signal or display to several audiences, asking whether Naim rushed this e-book to display an advantageous move among Islamic State leadership and other Indonesian competitors in Syria, for example.

Potz (2023) explored voluntary "costly signals" in religious communities, where he suggested it may have been assumed people who perform costly signals in a religious community are required to accomplish these rituals to be accepted into the group. There are other motivations driving costly signals, however, that are not required by the group, but nonetheless are regarded as costly and valuable, he wrote. Potz characterized these voluntary signals or displays as "structurally empowering" because of how it might influence the group's perceptions of whoever is signaling these costs. While required "costly" signals communicate commitment to that religious community, displaying or signaling a voluntary cost could improve or raise someone's reputation or standing within that community. Potz referred to Toland (1988) who wrote about this legitimation of power as something to be "thought of as an ongoing communication" process. In this context, that ongoing communication was arguably directed at Islamic State leadership and other Indonesian personalities, as much as it may have been directed at Western counterterrorism watchers.

3. Technical Behavioural Content Analysis of Naim's *Teknologi* Chapters

Technical assessments of known and unknown cyber offenders generally start with some characterization of an actor's technical knowledge. We are talking about his or her *native* knowledge, which is experiential and learned, as well as his or her *researched* knowledge, which is knowledge that would be searched for immediately on Google, or in some other manner because the offender is unfamiliar with that tool, for example.

While we cannot know if Naim had native knowledge then or at some point in the past of some of the techniques and programs he wrote about in his e-book, we can question why he included chapters that suggested he demonstrated these step-by-step techniques, when the screen shots found online in this paper indicated he repeatedly did not demonstrate those steps.

Generally, Naim's chapters on hacking read much like an introductory outline of different anonymizing techniques and some of his general opinions on hacking, for example. Naim's chapters throughout a section called *Teknologi* are increasingly filled with screen shots taken from companies and other users online who created those visuals with programs. Because readers see these screen shots accompanied with written instructions, most readers would probably believe that Naim is likely performing these steps on these programs and taking shots. Because of the length of the section *Teknologi*, we will be focusing on content examples that help frame Naim's suggested level or degree of *native* and *researched* knowledge.

3.1 Naim's Plagiarized Screen Shot Tutorials

The examples included below are questionable because there was likely no need for Naim to plagiarize these screen shots, as most of the examples are rudimentary demonstrations; Naim could have simply replicated the same tutorials he appeared to have found online. Further, the examples that appeared to have been plagiarized even include instructions such as entering a username and password, which are arguably laughable when considering that the presumed targeted reader for Naim among the broader Indonesian carding and cybercrime community would have been familiar already with many of these platforms and tools. If we argued that Naim was using other existing content online for his screen shots for operational security, so that he does not include any identifying content, we would have to argue that what he includes in some chapters for the Android may suggest that he is more comfortable using an Android smartphone, which starts to shape his technical profile.

3.2 VPN/OPENVPN

In this early chapter, Naim began including screen shots from what appeared to be other users or content from companies online, rather than demonstrating those steps himself. Naim wrote about calibrating a proxy service like OpenVPN to anonymize yourself online and how important safety is. What appeared to be a plagiarized screen shot demonstrates how a user would set up the OpenVPN installation client and then connect (see **Figure 1** and **Figure 2**).

Naim included the screen shot in Figure 1 in his e-book, which resembles the same screen shot in Figure 2 found by the author in a Google search. The numerous screen shots of OpenVPN and vpnbook as a free proxy vpn service are just informational, helping readers pick a free and secure option among several choices.

Figure 1: Naim's included screenshot of completing an OpenVPN profile installation

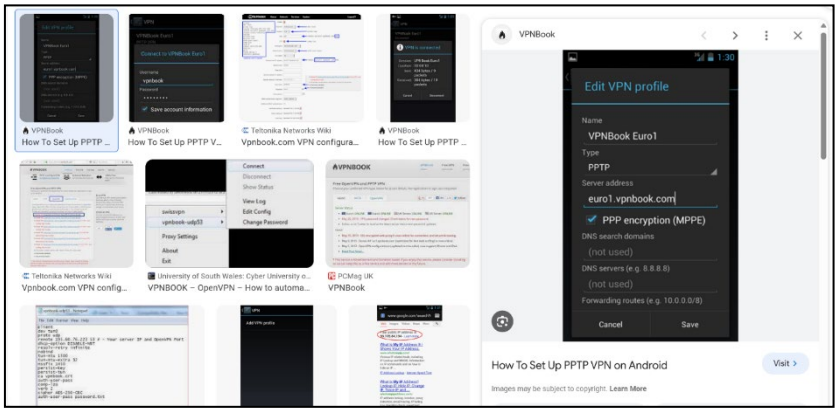

Figure 2: Author's Google search return including the same screenshot

3.3 SSH/OPENSSH

In this chapter, Naim discussed using a Secure Shell Protocol (SSH) cryptographic tunneling program over an unsecure network. Again, Naim used screen shots from existing content online from commercial sites, including screen shots that share some of a desktop Windows background that is likely not his. The same screen shot was found online among initial search results (see **Figure 3** and **Figure 4**).

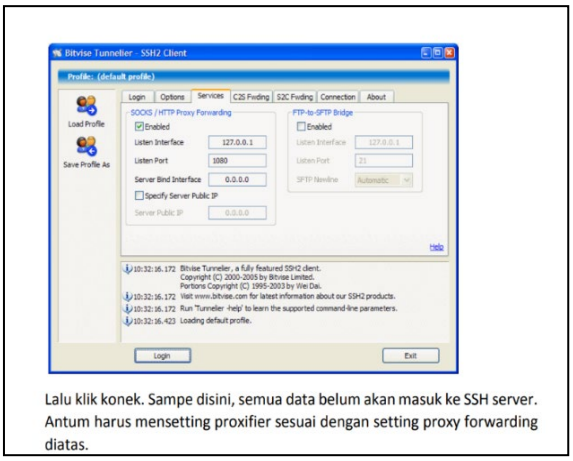

Figure 3: Naim's included screenshot of the connecting with an SSH2 client

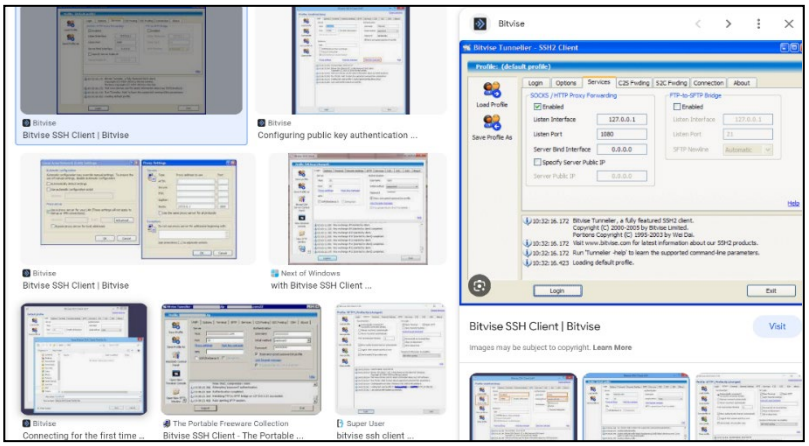

Figure 4: Author's Google search return including the same screenshot

Naim did include additional screen shots in this chapter that demonstrated setting up an SSH tunnel application on an Android, where even in Naim's written content below the screen shots he included port forwarding and setting details for calibrating that application. Again, Naim uses a screen shot from existing content online, in fact, content posted online by another Indonesian-language user on a blog site. The same graphic including the same screen shot that included an Indonesian-language advertisement in the screen shot was found on an Indonesian-language blog detailing the same technique for setting up an Android IP proxy (see **Figure 5** and **Figure 6**).

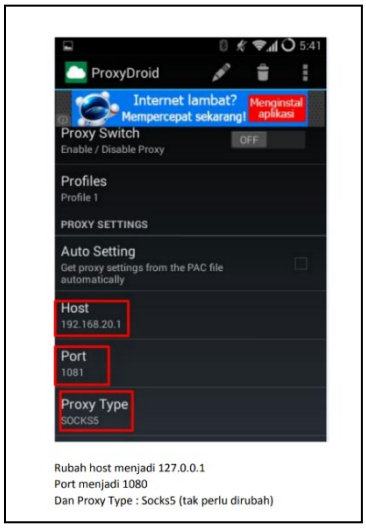

Figure 5: Naim's included screenshot setting up a proxy IP on an Android smartphone

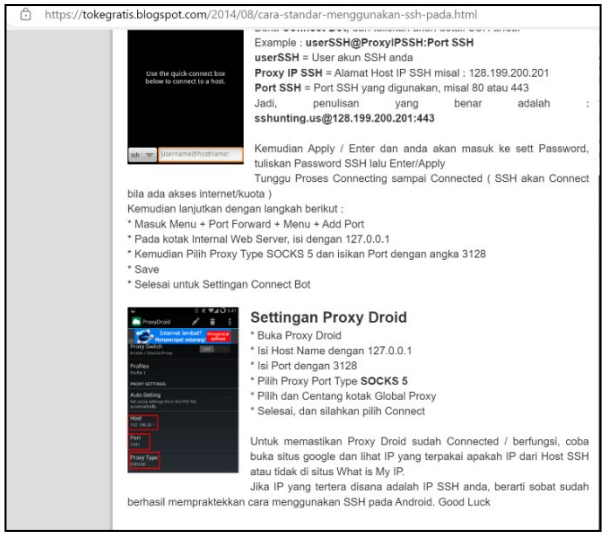

Figure 6: Author's Google search return including the same screenshot from an Indonesian-language blog

3.4 SQL Injection

In this chapter, Naim included an unreferenced screenshot from a blog article published in approximately 2012 (see **Figure 7** and **Figure 8**). While we do not know how Naim searched for this content, the same content is largely still available online when searching for the program names in screen shots that Naim included. There's limited uniformity to the screen shots included throughout these chapters, which suggests that Naim continued to plagiarize these screen shots from other unknown users online. In some screen shots, there are English-language text in different color fonts added to the image. Some of these screen shots included data that could be identifying that appeared simply written over with a marker rather than a highlight to redact that line of text.

Figure 7: Naim's included screenshot demonstrating use of the SQL Poizon tool

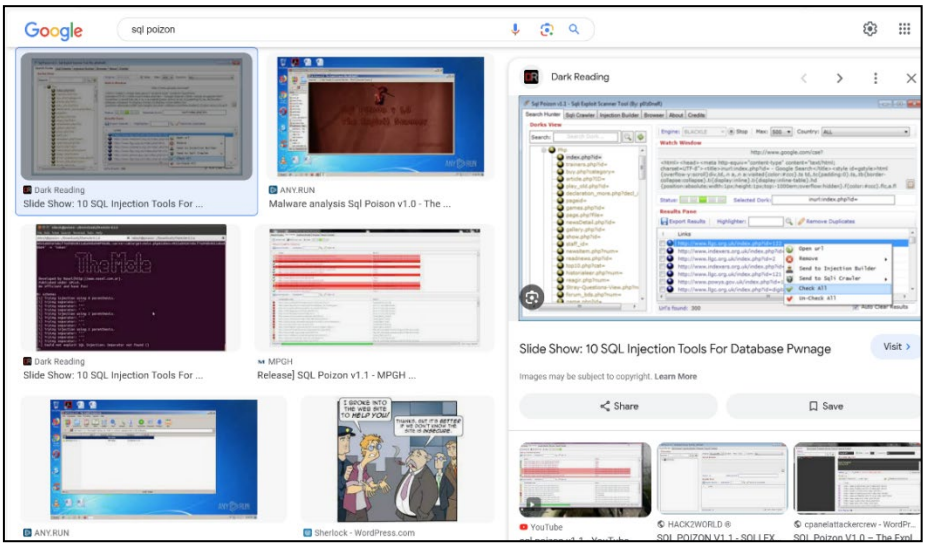

Figure 8: Author's Google search return including the same screenshot

3.5 Naim's Possible *Native* Technical Knowledge

We evaluate an offender's degree of native technical knowledge by examining what we know about that offender's study and other experiences with tools, for example. When there is limited information about what an offender has studied or practiced, we then consider how that offender discusses tools or techniques and what he or she chooses to demonstrate or operationalize in some kind of attack setting.

3.6 Proxy

Naim in this chapter explained what a proxy is and how there are weaknesses to using a free proxy service, rather than paying for a proxy that is not shared and is more secure. When Naim did appear to demonstrate the steps outlined, the process generally involved visiting the website on a desktop or mobile device that provided details on your IP address.

3.7 Socks/VIP72

In this chapter, Naim wrote extensively about both applications, including nuances, such as if you use Microsoft Proxy Server, then you do not need to install WinSock Proxy on the computer you are using, for example. Naim explained how the SOCKS proxy server can relay data safely between the sender and receiver and the connecting server. He noted that SOCKS version 5 added an additional step where each stage of that relay requires authentication. When we see this kind of explanation, there are suggestions that Naim is simply more comfortable writing about this topic because he is experienced using SOCKS, for example.

3.8 Cara Hacking Dan Carding

In this chapter, Naim wrote that he wanted to focus on some of the more common techniques for hacking and carding. First, Naim discussed Structured Query Language (SQL) injection. Naim characterized a SQL injection as a method to "open" a database to collect information in the database as needed. Naim suggested various software programs that could be used to support that technique. Second, Naim talked about exploits, such as Remote Access Trojans (RAT) on mobile phones, that enable collection on the host of that device.

Third, Naim described sniffing or packet sniffing as using a virus keylogger for example to catch packets "on the fly" that could include communications or other important data.[1] Fourth, Naim wrote about cache injections, which is a method he wrote of manufacturing hidden caches of data in files, which he described as a "very easy" technique. Fifth, Naim wrote about Domain Name Server (DNS) poisoning, which he described as a "simple" technique for reconfiguring the origin host DNS to manage control over traffic to the redirected DNS. Naim explained all these techniques in understandable contexts for what appear to be introductory technical readers who may have been unfamiliar with these techniques previously.

[1]Ibid., 90-91

3.9 Web Scam/Scampage

Naim wrote extensively in this chapter about the various *webscam* techniques, including how to manipulate Facebook account domains to trick people. While Naim did include a screen shot of an example of a falsified PayPal URL, this chapter includes lengthy background and plain language examples of how to set up *scampages*.

3.10 Metode Carding

Naim's subsequent chapter on carding methods is even lengthier, organized by platforms where the reader could card victims, such as PayPal and Western Union. Naim included written details in this chapter that describe options for what to input into various platforms to complete illicit carding transactions successfully. The notes Naim included for several listed sites strongly suggested he has some experience using these sites for carding. For example, on a skateboarding clothing site www.draven.com, Naim wrote that the reader can use the shipping address for the billing address and that the reader does not need to use Socks/VPN for this site (see **Figure 10**). There are ten pages of these sites with notes.

3.11 Metode DDOS

Naim in this chapter provided generally available information about Distributed Denial of Service (DDoS) attacks. Naim did include a screen shot of his famed botnet @bahrunnaim_bot and profile photograph as a method of using a botnet to flood a network, however, just above this part of the chapter where Naim wrote about command prompt as another method in Windows, Naim again plagiarized a screen shot demonstrating this method (see **Figure 11** and **Figure 12**).

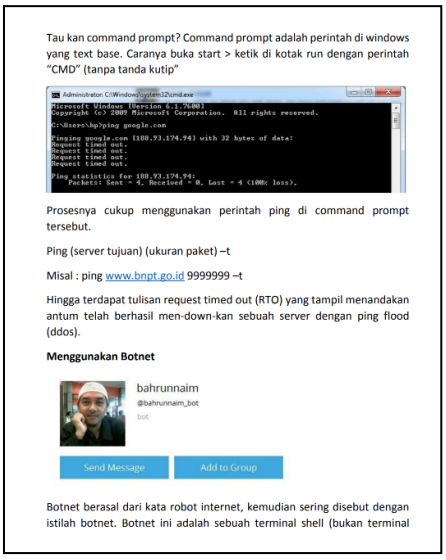

Figure 11: Naim's included screen shot for a command prompt function in Windows

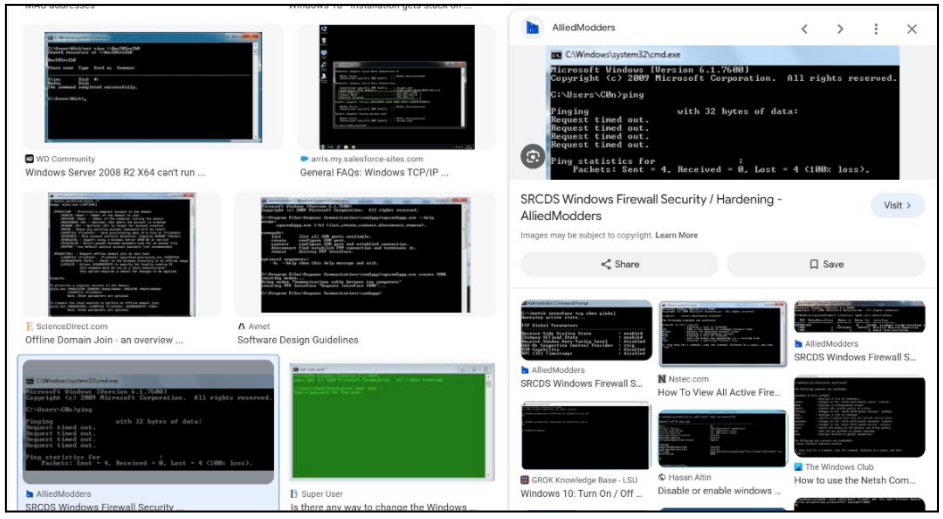

Figure 12: Author's Google search return including the same screenshot

3.12 Naim's Possible *Researched* Technical Knowledge

We evaluate an offender's degree of researched technical knowledge by examining what that offender claims to be able to do related to observable or known experience or training. The preference is to see an offender's behavior regarding a tool or technique, so we can observe either how they demonstrate a tool or technique or what kind of research is required for them to educate themselves on how to use that tool or technique.

For example, if we are observing an administrator who has responsibility for using Powershell in his or her position, but this administrator appears to struggle to appropriately use Powershell and often asks others for help or searches elsewhere for information on how to use Powershell correctly, then that administrator's knowledge of Powershell is likely researched more than native, and we now have some grounding for their technical aptitude or profile. The examples below just based on observation may suggest that Naim has limited researched knowledge, but what does appear to be researched are rudimentary topics that also include some examples of plagiarized screen shots.

3.13 Persiapan: Anonymous

Naim explained early in this chapter that he is trying to educate readers on how to avoid being "tapped" or "bugged" by others online, calling this chapter "preparations". Much of this chapter included Naim writing much like a summary on the hardware used to locate or identify people, such as Global Positioning System (GPS) or the IMEI on a phone. While we are speculating, Naim was likely killed because he did not anonymize appropriately.

3.14 *VPS*

Naim wrote in this chapter about Virtual Private Servers (VPS), such as the benefits of a continuous proxy infrastructure. Naim included a screen shot from a CentOS Webmin version. While the screen shot Naim included was not found during an open-source search, arguably Naim would not want to include the details on his VPS in a screen shot. The open-source search on Google for a similar display from a CentOS Webmin version included many similar screen shots like the one Naim included.

3.15 Google Dork

This 15-page chapter is the longest in Naim's e-book sections on hacking and carding. Most of the pages included lists of search terms to "Google Dork" search for files if the reader has established access on a site or a server to search for files.

3.16 Naim's Only Shared Example of Conducting an Attack Himself

We have found that generally cyber personalities online will showcase or certainly claim some of their exploits or attacks. Part of that learning and teaching process within some of these communities is demonstrating how that offender accomplished a technique and then providing some version of that tool to others so they can do the same. These are reputational displays or signals; however, this is the only example Naim includes in his entire e-book and dozens of chapters about hacking.

3.17 Exploit

In this chapter, Naim discussed the Remote Administrator Trojan (RAT) virus and how to launch this virus from various programs. Naim described how one method of executing this virus is through a website, where the victim sees what appears to be a warning message when they visit the website with a button to return to "safety" to avoid malware on that website. When the victim clicks on the button to return to safety, the virus starts downloading. Naim included a screen shot of an example, which identified www.hendropriyono.com as a malicious site. Naim did not include any further commentary on this website example, but that name is commonly associated with the name of an Indonesian general accused of abuses in East Timor.

In this same chapter, Naim referred to himself as the writer "*penulis*" conducting one of these attacks, for the first time in his e-book. Naim wrote that he remembered one time where an Indonesian counterterrorism officer from a cybercrime division named Roberto had difficulty printing an investigation document. Naim wrote that he "pierced" Roberto's account and observed Roberto's issues with the printer. Roberto's operating system ultimately crashed. Naim wrote that he believed the counterterrorism agency likely kept a backup of system files for Roberto's operating system and other accounts. Naim wrote that he forgot to write a script that would have automatically wiped all the files on Roberto's account.

4. Discussion

This practitioner's paper applied a content analysis of Naim's manifesto chapters on hacking in the context of *native* and *researched* technical analytical frameworks. These are practiced technical analytical frameworks of cyber behavioral analysis that have been applied in many instances, usually involving limited information on known and unknown offenders. We can start to baseline Naim's experiential technical knowledge and capabilities not only based on the content he chose to write about, but demonstrably how he wrote about that content, in contrast to areas he did not write as much about or did not seem comfortable writing about. Additionally, we can gain some sense of Naim's abilities based on the applications and software he chose to write about, whether he demonstrated or plagiarized those tutorial screen shots.

Based just on publicly available information, we have no known record of any instance of Naim conducting computer network operations against any individual or organizational network, other than the story in his manifesto of gaining unauthorized access to an Indonesian counterterrorism official's laptop account. By his own account, he had limited privileges and questionable scripting. Naim appeared to plagiarize most of the tutorial screen shots he included in his manifesto. Randomly sampling one of the tutorial screen shots or diagrams Naim included in another section of the manifesto on bomb making that appeared to include Naim's notes, also appeared to have been plagiarized from another user's content found online during a Google search.

This paper cannot answer why Naim chose to create an e-book rather than communicate this same information the way he had been sharing information on encrypted platforms, or rather than creating video content like many of his peers in the Islamic State. By the time of his death in June 2018, YouTube was already brimming with online tutorials for every kind of hacking technique and platform imaginable; in fact, Naim appeared to plagiarize many of his screen shots from content hosted on Google platforms. Naim shared information about bomb making and weapons on his encrypted platforms, but routinely had to create new accounts in response to his accounts being suspended or banned; perhaps there was greater redundancy in an electronic book that could be more easily shared among broad and niche Indonesian communities and audiences of interest for Naim.

While Naim referred to himself in his manifesto as "just a writer", perhaps he imagined himself to be an Islamic scholar of some note, or he wanted some pedagogical role. This paper suggests it could be all those reasons and more, but arguably Naim's technical pedigree was widely embellished or misunderstood by counterterrorism and cyber analysts. This paper suggests there is greater opportunity to diffuse cyberterrorist influencers by materially highlighting their surprising lack of technical experience and knowledge, rather than simply categorizing them as another concerning terrorist personality. There is a growing world market of cyber talent who even with extremist interests would likely find Naim's plagiarized tutorials laughable.

References

Arianti, Vidia, "Aman Abdurrahman: Ideologue and 'Commander' of IS Supporters in Indonesia," *Counter Terrorist Trends and Analyses* 9, no. 2 (2017).

Arianti, Vidia, "Cybercrime: Financing Terrorism in Indonesia," *RSIS Commentary* 159 (2019).

Baenzer, Marie, Hotspot analysis: use of cyber tools in regional tensions in Southeast Asia, Center for Security Studies, Zurich (August 2018), Cyber-Reports-2018-05.pdf (ethz.ch).

Bliege, Bird, Rebecca, and EricAlden Smith. "Signaling theory, strategic interaction, and symbolic capital." *Current anthropology* 46, no. 2 (2005).

DeAndrea, David C. "Advancing warranting theory." *Communication Theory* 24, no. 2 (2014).

Donath, Judith. "Signals in social supernets." *Journal of computer-mediated communication* 13, no. 1 (2007): 232-233; "Signaling Identity." *Sociable Media Group* 10 (2007).

Gunaratna, Rohan, "Mastermind of Terror: The Life and Death of Bahrun Naim," *Counter Terrorist Trends and Analyses* 10, no. 10 (2018).

International Institute of Counter-Terrorism, "IS-Supporting Hacktivists in Southeast Asia", Reichman University, June 2, 2019, 10, IS-supporting Hacktivists in SE Asia v1 (ict.org.il).

Joscelyn, Thomas, "Indonesian authorities hunt Islamic State operative's cyber recruits," *FDD's Long War Journal*, April 18, 2017, www.longwarjournal.org/archives/2017/04/Indonesian-authorities-hunt-islamic-state-operatives-cyber-recruits.php.

Kassim, Y. Z., "The Jakarta assault: pre-empting the rise of IS Indonesia," *RSIS Com mentary* 17 (2016).

Lang, Martin, Radim Chvaja, and Benjamin Grant Purzycki, "Costly commitment signals promote co-operation and sacrifice during intergroup conflict", (2023).

Liu, Christine M., and Donath, Judith. "Urbanhermes: social signaling with electronic fashion." In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pp. 1. 2006.

Mulia, Musdah, "Bahaya radikalisme dan kekerasan ekstrismisme," *AL-WARDAH: Jurnal Kajian Perempuan, Gender dan Agama* 12, no. 2 (2019).

Naim, Bahrun. *"Sebuah Perjalanan, Rahasia".*
Romadlan, Said, "The Discourse of Meaning of Jihad in Muhammadiyah Circle (A Hermeneutics Perspective)," *Komunikator* 11, no. 2 (2019).
Rozika, Weldi, "Propaganda dan penyebaran ideologi terorisme melalui media internet (Studi kasus pelaku cyber terorisme oleh bahrun naim)," *Jurnal Ilmu Kepolisian* 11, no. 2 (2017).
Schulze, Kirsten E., "The Jakarta attack and the Islamic State threat to Indonesia," *CTC Sentinel* 9 (2016).
Singh, Bilveer, "Southeast Asian jihadi leaders in the post-Marawi era," *RSIS Commentaries, CO18007* 16 (2018).
Taufiqurrohman, Muh, and Ardi Putra Prasetya, "A Rising Indonesian Jihadist Plotter: Bahrun Naim," *Counter Terrorist Trends and Analyses* 8, no. 11 (2016).