Understanding cybercriminals through analysis of penetration testing group dynamics

Rachel Bleiman
Department of Criminal Justice
Temple University
Philadelphia, USA
rachel.bleiman@temple.edu

Mollie Ducoste
Department of Criminal Justice
Temple University
Philadelphia, USA
mollie.ducoste@temple.edu

Aunshul Rege
Department of Criminal Justice
Temple University
Philadelphia, USA
rege@temple.edu

***Abstract*—Cyberattacks are a major threat in the modern era, yet there is a lack of information on how cybercrime groups think and operate. This paper aims to better understand cyber adversaries by analyzing penetration testing teams during the 2018 and 2019 National Collegiate Penetration Testing Competition, in which groups of students performed similar actions as cybercriminals, attempting to identify and exploit system vulnerabilities. Using penetration testing teams as an ethical proxy for cybercrime groups allows the researchers to study group dynamics as well as factors impacting the rationality of cybercriminals. Themes identified in manually coded interview transcripts are compared to the existing literature on cybercrime groups. Similar to what is established in the prior research, themes emerged in the interviews on the group structure and dynamics of each team, featuring elements of leadership, division of labor, the role of each team member, the presence of partners and subgroups, communication within the team, and interpersonal team member relationships. Other apparent factors that specifically impacted the bounded, or limited, rationality of the team members included setbacks and problem solving, the competition environment, stress, and issues with morale. This comparison of penetration testing groups with cybercrime groups allows for the development of a better understanding of the operations and rational thinking of a criminal organization, which may lead to a better understanding of how to prevent or defend against cyberattacks, such as by improving response times of the security team or by increasing the difficulty of penetrating the technical environment.**

Keywords—groups dynamics, cybercrime, penetration testing, bounded rationality

I. Introduction

With the prevalence of cybercrimes that are occurring in today's world, there is a need to better understand how those who commit them operate, so that society can better defend or even prevent such attacks from occurring. However, it is difficult to study cybercrime groups due to ethical concerns of observing the execution of cyberattacks. Fortunately, there is a similar group of people who perform comparable tasks to cybercriminals, yet they do so legally with no malicious intent. Penetration testers, or pen testers, are hired by companies to identify weaknesses and vulnerabilities in security systems so that their clients can be aware of areas that need improvement. To identify these problem areas, penetration testers often work as a team and operate on the offensive side of an attack as criminals do, to find and exploit the vulnerabilities of a computer security system. This allows the clients that hired the penetration testing team to gain awareness of where their security is lacking. Thus, cybercrime groups can be ethically analyzed through studying penetration testing groups instead.

The following points are the contributions from this work. First, this work demonstrates that cybersecurity events can serve as proxies for real cyberattacks. Second, this work discusses proactive cybersecurity measures to be implemented based on the findings of this study. More details on these contributions can be found in the discussion section (see section VII).

This paper analyzes group dynamics by comparing the known elements of cybercrime groups with the observed elements of penetration testing groups. Thus, the next section of this paper outlines the known elements of criminal groups including their composition, structure, and rationality. The following two sections provide more details on the current study and the methods used to collect and analyze the data. The results section then identifies the elements of penetration testing group dynamics found in the collected data. Then, the discussion section makes a comparison between the data on group dynamics from penetration testing groups and the established elements from cybercrime organizations, as well as identifies limitations of this study. Finally this paper concludes with the authors' closing remarks and takeaway thoughts.

II. Literature Review

There is not extensive work that examines the group dynamics of cybercrime groups, and even less works that use penetration testing groups, competition setting or otherwise, as a proxy for real cybercriminal groups. However, past work has qualitatively looked at penetration testing groups for the purpose of understanding and developing cybersecurity technologies. For example, Zheng et al. (2020) studied the processes of two penetration testing groups, finding that using visual representations of penetration testing paths help researchers better understand penetration processes [1].

While it is rare to use penetration testing competition groups as proxies for cybercriminal groups, it is not uncommon to observe more accessible cyber groups that mimic the behavior of adversarial cyber groups. For

example, one case study took place at a cybersecurity training held at Idaho National Library (INL), where researchers observed exercise teams to capture the shifting group dynamics in response to defense tactics used by opposing teams [2]. This particular study found that while the group members tended to start off by working on one task together, they later delegated specific tasks to individuals or sub-groups. Another study derived from the same INL training exercise argued that understanding adversarial behavior is a crucial element in developing the most effective preemptive cybersecurity safety measures [3]. A similar study used a cybersecurity exercise held at the North American International Cyber Summit (NAICS) to understand how cyber groups adapt and anticipate defense measures [4]. By observing cyber exercises in this way, researchers were able to better understand adversarial decision making, group dynamics, group structures, group cohesiveness, group response to conflict, and division of labor.

There exists a gap in current cybercrime literature that outlines direct observation of cybercriminal groups, and it is this gap that the current study begins to address. The following section will outline the ways that previous literature has explored the specific and theoretical factors that impact cybercriminal groups. Namely, the following section will look at the properties of cybercriminal group composition, division of labor, group structure, and the concept of bounded rationality.

III. Group Dynamics and Decision Making

A. Group Composition

The composition of a criminal group, including the membership process and the roles, factors into the dynamics and success of a group. A 2003 study [5] found that membership to a group is selected based on three preferences: high expected value to the group, personal familiarity, and a similarity to the existing members in the group; however, membership tends to be fluid. Once the group is formed, successful crime groups tend to develop a functional division of labor [6]. Roles and jobs are divided among the group based on individuals' specialties [6]. There may be specific individuals whose roles involve writing the exploits or malware that will be executed in an attack [6]. Other individuals may be in charge of finding vulnerabilities in targets' systems or develop and execute fraud techniques such as phishing or spamming [6]. Dependent on the structural organization of the group, there may be an executive that oversees the operations and roles of the rest of the group [6]. However, there is no established classification scheme among cybercrime groups, as their structures tend to vary by group, some are centralized while others are decentralized [7].

B. Division of Labor

Some groups, however, have developed a functional division of labor system. The main roles of a criminal network are the organizers, extenders, executors, enforcers, money movers, and crossovers [8]. The *organizers* are the ones who determine the actions of the group such as what crime will be committed and how it will be committed. The role of the *extenders* is to expand the criminal network by recruiting members. Next, the *executors* carry out the organizers' objectives and plans; they possess the specific skills necessary for the specific objective. For example, in a romance scam network, the executors are able to bond with, communicate with, and seduce the victims through fake online dating profiles [8]. Next, the *enforcers* protect the criminal network and make sure the victims cooperate by any means necessary, such as through extortion or blackmail. For example, in the case of a ransomware attack, enforcers may play upon the victims' fear of having their information leaked to guarantee the victims' compliance and payment [9]. Next, the job of the *money movers* is to transfer the money from the victims and return it to the criminal network. Finally, some criminal networks have a role for *crossovers*, which are people who work in, or have access to, legitimate governmental, financial, or commercial sectors, serving as inside sources. For example, in online human trafficking, someone with the role of the crossover may be able to provide documents that appear to be genuine to help convince the victim to travel to a specific location [8].

C. Group structures

Within the different group structure typologies are networks and hierarchies: two typical, opposing group structures. Network structures are usually more collaborative, and rely on mutual dependence within groups, even if they have diverging interests [10]. Contrarily, hierarchical structures involve unilateral decision making, wherein an individual actor defines problems, makes decisions, and dictates implementation [11]. While the emphasis on the "collective" in network settings diverges from the tiered hierarchical setting, research has found that there can be hierarchical unilateral decision making within network settings. Specifically, unilateral interventions at appropriate, opportune times within network settings can lead to overall successful group collaborative dynamics [12].

Furthermore, there exists different types of relationships or interdependencies between members of a group. A group may have unilateral interdependencies, which are relationships in which one team member influences all of the other team members [13]. There can be sequential interdependencies, in which one group member influences someone, who then influences someone else [13]. There are also reciprocal relationships, in which multiple members influence each other mutually [13]. A single group can contain all of these relationship types [13].

Although network and hierarchical settings can be successfully incorporated into one group setting, there are a number of risks posed by improper integration of the two settings. Namely, hierarchical decision making within network settings can cause incentive for opposition, weakening of negotiating position, and a reduction in collaborative learning opportunities [12]. However, these risks can be mitigated if groups use unilateral decision making to maximize win-win situations, promote healthier relationships, provide appropriate reactive action for failed

cooperation, and emphasize the true agency and power of networks.

Despite these risks, there could also be benefits of integrating network and hierarchal settings if done successfully. One benefit is regeneration, in which the rest of the network is not exposed or hurt if one member is compromised. Despite an instance of an exposure in the network, it can still function properly by simply making a replacement [14].

The incorporation of different network structures also brings to light the different conflict resolution tactics of groups. These group settings point to the different ways in which the larger group can be incorporated into both network and unilateral decisions. The proper incorporation of these techniques can generally increase overall comfort and satisfaction within groups [15]. Interactive decision-making leads to better support and learning opportunities for group members [12].

While the group structures of organized cybercrime groups are known, there is much less information on the personal group dynamics of cybercriminals, which increases the importance of understanding how they think and perform.

D. Bounded rationality

A main factor that impacts a group's performance is the bounded rationality of its members. Rational choice theory describes criminals' rational consideration of risks and benefits when deciding to commit or not commit a crime. An individual ultimately decides to commit a crime when they consider the benefits of crime to outweigh the risk of punishment [16]. This theoretical perspective has often been used to describe the behavior of cybercriminals, who weigh this combination of opportunities and limitations in the hacking process. Under rational choice theory, the criminal event is a deliberate act designed to fit the offender's unique needs [17]. Because of the individuality of offender needs, rational choice theory also has a crime-specific focus, meaning that the rational weight of risks and benefits are particular to the type of crime being committed [16]. The decision-making process that takes place within a criminal event is often made quickly with the expectation of more immediate results [17]. However, because this decision-making process happens quickly, it does not always result in the most rational decision. Satisfactory decisions might be made over optimal decisions. Thus, the rationality of offenders is bounded and imperfect. There is a wide array of factors that might contribute to this bounded rationality and make the decision-making process more difficult, ranging from logistical reasons, such as time constraints, to emotional or cognitive reasons, such as stress or fear [18].

IV. Current Study

To study a group of penetration testers, data were collected at the 2018 and 2019 National Collegiate Penetration Testing Competition located at the Rochester Institute of Technology in Rochester, New York. The CPTC mimics a real-world penetration testing engagement by creating a simulated version of a corporate network and tasking teams of three to eight undergraduate students to identify and resolve critical security vulnerabilities in the system [19]. This international competition requires teams to practice their technical skills to identify weaknesses, communication skills to explain technical concepts to both technical and non-technical audiences, and collaboration skills to work as a team to complete the task in the allotted time of about seven hours[19]. By the end of the competition, the teams must have a project deliverable in the form of a report of their findings [19]. Teams were directly observed during the competition and later participated in group interviews with the researchers. While the teams were required to stay within certain parameters to complete their task of identifying and mitigating security vulnerabilities, they were free to develop their own attack plans and delegate tasks in any manner of their choosing, including forming subgroups or choosing a leader. The current study seeks to further understand the group dynamics and rational decision making of penetration testers, including analyzing member composition and group structure.

V. Methods

The current study uses a qualitative approach to examine the group dynamics and their functionality within the penetration testing teams. Prior research in cybersecurity has found that using qualitative methods can help researchers develop a comprehensive understanding of complex hacking processes [20,21,22]. Additionally, using interviews in qualitative work can allow for researchers to tailor their questions and dialogue to extract valuable information about social phenomena [23].

The data of this particular study come from a series of interviews (n=18) with penetration teams from the 2018 and 2019 CPTC event. Each team consisted of about six people. Although penetration testers hack systems legally and therefore do not commit crimes, they must simulate the thought processes of a cybercriminal with malicious intent. Because pentesters must foresee the possible directions to be taken by a cybercriminal, their objective is goal-oriented, just as cybercriminals carry out attacks with a specific goal [24].Thus, pentesters serve as a good proxy to cybercrime groups, and although the two are not identical, examining pentesters can give some indication or insight into cybercrime groups. As rational decision makers, both cybercriminals and penetration testers experience bounded rationality, which can contribute to imperfect decision-making and affect overall group performance. The commonality between the two groups in their goals and rational thought processes supports using pentesters as an alternative to studying cybercriminals.

The interviews with the penetration testing teams lasted at most an hour each and provided CPTC participants the opportunity to detail their experiences in the competition, including their particular experiences related to their group dynamics. Each interview used the same set of questions to ensure consistency; however, some of the respondents' answers received unique follow-up questions. Some of the

questions that each team were asked were, "What are each of your individual roles/skillsets?", and when discussing challenges they faced, "How did you overcome those hurdles?". The interviews were subsequently transcribed and coded. Each researcher used a grounded-theory approach to develop coding schemes [23], where the analysis was driven by themes identified in the data. These coding schemes were checked by the other researcher to ensure consistency in coding across transcripts. Using this systematic approach, large and consistent themes emerged as researchers worked to identify appropriate codes that best illustrated the objectives of the current study. Through this process, the researchers overwhelmingly found the same set of codes.

VI. Results

The researchers identified themes regarding group dynamics from the team interviews following the 2018 and 2019 penetration testing competitions. These overarching themes included the *group structure and dynamics* of the team, as well as *factors that impacted bounded rationality*. The following sections will detail these themes (see Table 1), which highlight how a group operates while completing a task to penetrate a company's network.

Table 1: Themes of pentesting groups

Group Structure and Dynamics	**Factors impacting Bounded Rationality**
Leadership	Problem Solving/Setbacks
Division of Labor	Environment
Roles	Stress
Partners/Subgroups	Morale
Communication	
Relationships & Bonding	

A. Group structure and dynamics

Throughout the penetration testing competition, the group structure and dynamics of each team featured elements of leadership, division of labor, the role of each team member, the presence of partners and subgroups, communication within the team, and interpersonal team member relationships.

a.) Leadership: A recurring theme that was revealed in the post-event interviews was the presence of leadership or a hierarchal structure within the teams. Of the 18 teams interviewed, 10 teams revealed that they had a predetermined team leader or co-leaders, whose roles varied among the teams, but whose responsibilities primarily included coordinating and distributing work to other team members, prioritizing individual tasks, keeping team members focused, and overseeing documentation. This leadership represents a unilateral relationship, as discussed in the literature review. Team leaders or managers typically also assisted team members on individual tasks. For instance, one team leader stated, "I was a second set of eyes to help push the other [team members] along if they started feeling like they hit a wall, and if so, a second pair of eyes can confirm that maybe we should move on and continue, or if this is really worth spending our time on". This competition also saw teams with co-captains, or team members assigned to supplement and aid the captain, which represents a reciprocal relationship between the co-captains, and a unilateral interdependency between the leader and the other group members. Other teams with only reciprocal relationships were still able to function well without a designated leader or captain. For example, one team stated that "we didn't have a clear hierarchy or leadership, but everyone really understood well what they had to get done and they were doing that".

b.) Division of labor: Another theme that was identified was the way in which individual tasks were assigned and divided among the team members. Teams expressed a range of methods they used when dividing the work and tasks among teammates. Some groups had leaders who assigned tasks to team members, while other groups had the freedom to choose their own jobs and responsibilities. For instance, one team explained that "each member of the team has a lot of free reign. There's not a whole lot of like, 'you need to get off that box and get on this.' We generally kind of trust each other to know when you've reached your limit, or when you need to switch off and we handle that". To contrast that, one team noted that "We did whatever [the team captain] said to do". Each team member's independent task depended on their skillset, whether it was chosen by them or assigned to them, such as one team who explained that "we assigned those [jobs], or we all chose what we'd like to work on or what was best for our skill set to start off with, and we worked on that system."

c.) Roles: The range of skills necessary to complete a successful penetration test resulted in various roles for the teams. Skill sets ranged from technical capabilities to business and organizational skills, which were required for the various components of the penetration test. Each team member had a specific skillset, which influenced the role they had on the team. The recurring skills and roles that emerged among the teams included technical skillsets in Linux, Windows, software scripting, networking, security engineering, and penetration testing, as well as social skillsets on the business and organization side. Oftentimes, a single person would be assigned a specific task and that would become their role, such as continuously performing reconnaissance or searching for vulnerabilities to exploit. These roles were typically based on the team members' skillset. Depending on the roles, certain team members would work closely with each other. For instance, someone whose role was to find vulnerabilities, needed to maintain close communication with the person performing reconnaissance to effectively complete their job. A member from one team stated, "I was mainly focused on finding exploits or vulnerabilities, going off of [my fellow team member's] reconnaissance throughout the engagement".

d.) Partners/subgroups: While team members had their individual skillsets and thus individual roles and jobs, there were times throughout the penetration test in which group members worked with a partner or subgroup to complete a task that required multiple skills. When a range of skills were needed for a particular task, either a different team member would take over that task, or multiple team members would

work on the task together. For instance, one team reported that "I worked very closely with [team member] six on using the tools set up by [team member] one and [team member] three to actually get shells, get root access, get stuff we weren't supposed to get." Some groups would even sit together strategically to be close to other team members with whom they worked together often. A member from one such team explained that "because we all had different skill sets, […] if someone […] needs some question answered or help with that directory, I can go check on it".

e.) Communication: Successfully working as a team required communication among group members, which became a relevant theme to the group dynamic and strategies of the teams. Some teams even used specific tools to facilitate communication within the team, such as one group who reported that "I think one […] of the most valuable skills in this kind of field, regardless of whether it is offensive or defensive, is being able to communicate […] We had a tool that allowed us to let each other know where we were working and not to step on each other's toes. So that was something that was steady throughout the whole competition and we were in constant communication". Keeping open communication was a key factor for teams for several reasons, including team members avoiding any unnecessary repetition of work, avoiding missed opportunities for exploits, , or helping other team members complete their task. Teams also reported that communication was important because "having a fresh mind or fresh eyes to something always helps with things [when] you're just stuck".

f.) Relationships & Bonding: The vast majority of the teams had at least a few members who knew each other prior to entering the competition setting. Additionally, many teams identified these existing relationships as factors that helped influence their group dynamics. For example, one team member stated: "Spending the time together helped us really get to know each other and be able to plan and be flexible and know who to talk to when we're actually in the setting." Similarly, another team member discussed how past attempts at problem solving prior to the competition helped the team work together during the competition: "Also, for training, we used to train together, so we would all train on … the same environments … to prepare ourselves as a team … to manage problems ... that [would] come up. So that was very beneficial."

While there were many bonds that existed prior to the competition, teams also discussed how the competition itself served as a setting where new bonds could be created within teams. For example, one team discussed how working together allowed them to build relationships while developing skills: "Working as a team on a security project that's offensive is a very, very valuable and [a] new experience for me and for the team dynamics or working technically and non-technically on security related things was a big gain." Another team identified that the new bonds within the team were comparable to winning the competition itself: "the real prize was the friends you made along the way."

In addition to the group structure and dynamics, the researchers identified themes from the group interviews that highlighted some of the factors that impact the bounded rationality of the teams.

B. Factors impacting bounded rationality

Teams discussed several factors contributing to their bounded rationality, affecting their decision-making processes throughout the competition. Such factors included setbacks and attempts at problem solving, the competition environment, stress, and issues with morale.

a.) Problem solving/setbacks: In any group task, there are going to be setbacks and thus, the need for problem solving. This requirement to think quickly to problem solve any hurdles often affects the rationality of decision making. The following challenges show how quick problem-solving affects rational thinking. A common difficulty and struggle that the teams faced in the process of the penetration test was working within the given time constraint. For example, one team reported that "we couldn't actually spend the required time needed in that critical section of the assessment, so it was just like ok … what have we found so far that we can go off of?"

Other environmental setbacks or challenges attributable to the competition aspect included stress and lack of sleep. One group noted that they wished they had slept more, saying that "didn't really have much" and that because of that, "approaching night I think most of us were dead [while] working."

Yet another penetration testing setback that the teams often faced was due to the lack of preparation for certain situations. One team noted that "the few mistakes that we may have made were just due to on-the-spot decisions where we had to improvise and... basically situations that are difficult to prepare for unless we had prior experiences". Teams often adapted to such setbacks by continuously running reconnaissance to look for any changes in the network that arise.

Another challenge that teams needed to adapt to was becoming stuck on one particular issue. For instance, one team realized that "we fell into a lot of rabbit holes. And when we're walking through the same FTP server trying the same credentials over and over to log into something, I think something that I definitely needed to do was just take a step back, say 'this isn't going to work' and try something else".

These unexpected and time-sensitive decisions link back to the concept of a bounded rationality discussed in II.C, in which the team members cannot effectively weigh the risks and benefits of each possible option, resulting in teams making less than optimal choices throughout the duration of the competition.

b.) Environment: The teams spoke about the competition's environment in two distinct ways. First, they described the ways in which the general setting of the competition, particularly as it related to client interactions, affected their group dynamics. One team member described the demanding nature of the environment due to the constant client interruptions: "the competition environment here was

much more fast paced in terms of demanding those things from you and demanding that you be flexible and respond promptly than I had encountered, so I learned a whole lot about what it's like to be in that kind of business environment even if it was just a simulated business." Similarly, another team member noted that the client interactions would involve heightened emotions, testing the patience and tenacity of the groups.

While the teams were affected by the overall competition setting, they also reported some team-specific environmental factors that contributed to their group dynamics throughout the competition. One team member described the general angst experienced by the teams throughout the competition, pointing to "the nerves, and the excitement, and the endorphins and everything happening all at once." Some teams had positive experiences in this environment, such as a team who reported that "this is a good kind of work environment, and this felt motivating, this felt good to work in, constructive to work in.." Other teams did not reflect positively on their experience working in the competition environment. Regardless, it is likely that a team's positive experience with the environment has a more positive impact on the team's bounded rationality.

c.) Stress: Related to the competition-based environmental factors was the general stress felt by the teams. Many teams pointed to the client interruptions as a source of stress for their members. One team discussed their difficulty dealing with clients and how it related to their overall group dynamics. They reflected on the need to prepare for the heightened levels of emotions associated with speaking to the clients and how it distracted them from balancing their group dynamics and tasks. Working while feeling high levels of stress can impact the rational decision-making process, resulting in a bounded rationality. Another team member discussed how their team was able come together to counteract this source of stress: "I believe the team took [the stress] really well where we either let it roll right off of us or brushed it off. Not allowing any kind of fissures within the team or any arguing to take place."

Another source of stress unrelated to the client interactions had to do with the technical aspect of the competition. For example, one team discussed their frustrations associated with using tools: "at some points [I] get frustrated with using a bunch of tools that I don't necessarily understand." Another team discussed technical stressors associated with their plan of attack during the competition: "Initially it was somewhat frustrating because of a few technical issues that occurred. But after that we were able to pick ourselves back together and continue on, even with some issues. From there on, it was... trial and error for most of the time; sometimes things worked, sometimes they didn't." Lack of knowledge about key technical factors can result in a bounded rationality, as properly weighing the risks and rewards of an action is not possible when there are unknown or misunderstood elements in the equation.

d.) Morale: When describing their fluctuations in morale during the course of the competition, many teams discussed how they felt a major boost in morale when they overcame any setbacks or made any important findings. For example, one team discussed how they would second-guess the effectiveness of their methods during setbacks until they were able to overcome them: "Emotionally it was a roller coaster. I would say it was fine. But when you get that roadblock you're definitely questioning if you made the right decisions. But once you get past that roadblock and you find what you're looking for, that's when it goes away." Similarly, another team member discussed the overall morale boost within the team when things went according to plan: "Just to expand how the morale boost was especially good: because we had theorized that we could [get] the initial foothold by using a variation of a weak password, and we had found this weak password for the event as part of the competition … we had theorized that a certain change would make it usable, and that did work, so being proven right … was a good morale boost for the team."

Contrary to these experiences of morale boosts, teams also experienced moments of discouragement when things did not go according to plan. For example, one team discussed how they almost felt like giving up after a rule violation landed them with a 1.5-hour penalty: "There was kind of a lack of care. I feel like I can say for myself because of the situation we were put in because of the breach. I feel like we were already at a huge disadvantage and it was hard to be more motivated." Another team discussed their lack of motivation that came about when they did not have the needed skillsets for a task: "It just gets very frustrating when you just can't figure out how something works, and you can't even determine if it is working. And if you don't have the prior knowledge of expecting this and playing with it, setting these things up, it's just... you start throwing things at it and you start expecting it just not to work. So, you […] lose the motivation to keep poking at it." This lack of motivation and low morale can also contribute to a bounded rationality, making it harder to weigh the risks and rewards to make the optimal, rational decision throughout the competition.

VII. Discussion

While it is difficult to study or observe a cybercriminal group execute a malicious act of breaching a network due to its unethical and risky nature, penetration testers serve as a possible replacement from which researchers can learn. In this study, the penetration testing groups showed several commonalities as to what is known about criminal groups, such as the types of group structure, including a network versus a hierarchy, and the group composition, such as the roles and skillsets of each member. Because these two types of groups perform with the same task in mind, studying penetration testers and learning how they function may give insight into the operations of a cybercriminal organization. Studying penetration testers revealed information about team structures and strategies that are otherwise not known about malicious cybercrime groups, such as how they communicate with each other or how they solve problems. Thus, by comparing penetration testing groups with cybercrime

groups, researchers can develop a better understanding of the operations of a criminal organization, which may lead to a better understanding of how to mitigate the effects of, prevent, or defend against cyberattacks.

This study has limitations regarding the data source. The competition aspect of the CPTC, as opposed to a typical penetration test in the industry, may change some of the dynamics of the penetration testing groups, including different motivations or stressors of each team member. For example, the competition teams were motivated to win the competition rather than complete their job duties. Also, the stress associated with the competition may differ from industry penetration tests. Furthermore, the competition teams have less penetration testing experience than professionals in the field, which may impact how they operate. Additionally, while this study uses a penetration testing team to potentially learn more about cybercriminal groups' dynamics and operations, penetration testing is not meant to be malicious, even though they are attacking a network. Therefore, it is not an exact match to malicious cybercriminal groups, and the team members in the penetration testing group have different motivations to complete the same task as the team members in a malicious cybercrime group.

Despite these limitations, this paper demonstrates how cybersecurity events can serve as a stand-in for real cyberattacks, and how pen testers can serve as proxies for cybercriminals' organizational dynamics and bounded rationalities. Further applications across different cybersecurity exercises and team structures may help generalize cybercriminals' operations and factors influencing their decision-making.

These findings encourage proactive cybersecurity measures to defend against cyberattacks, specifically by designing security in a way that targets the bounded rationality of the adversaries. Heightening the security within the technical environment will directly impact bounded rationality by requiring the attackers to adapt and problem solve. Another method to affect attackers' bounded rationality is to decrease the response time of the security teams, so the cybercriminal groups experience tighter time constraints. Targeting the attackers' bounded rationality may cause them to make more mistakes, which could induce stress or lower morale, further contributing to their bounded rationality and causing additional missteps, as seen in the experiences of the penetration testing teams.

VIII. Conclusion

This paper presents pertinent aspects of group dynamics that occur during a penetration test competition, which can be used to learn more about the operations of cybercrime groups. The results showed similarities between the observed elements of penetration testers and what is known about cybercrime groups, as well as offering further information learned from the penetration testing teams, which gives insight into the minds and operations of the malicious groups. Given the heightened threat and frequency of cyberattacks today, it is especially important to understand how cybercrime groups think and operate, so that steps can be taken to create defensive measures, with the hope to diminish the success of attacks and reduce instances of victimization.

To do so, future research can investigate how organized criminals use pentesting team recruitment strategies, such as advertising and interviewing, to gain new members. Further research can examine other cybersecurity events to confirm whether these group dynamics are similar and can be found in other settings. Further research can also focus on bounded rationality in the context of penetration testing. This may confirm the factors of group dynamics that impact bounded rationality that were found in this study or identify additional factors that influence the decision-making processes of those involved in cyberattacks, potentially identifying ways to limit, hinder, or interfere in their rational decision-making processes. Finally, research can examine the extent (strength and direction) to which these factors of group dynamics impact bounded rationality and how these factors may even work together to compound the impact on rationality and decision-making.

References

[1] Zheng, S., Wu, Y., Wang, S., Wei, Y., Mu, D., He., H., Han, D., Liao, J. & Chen, H. (2020). PTVis: Visual narrative and auxiliary decision to assist in comprehending the penetration testing process. IEEE Access, 8, 194523-194539.

[2] Asadi, N., Rege, A. & Obradovic, Z. (2018) Assessment of group dynamics during cyber crime through temporal network topology. In: Thomson, R., Dancy, C., Hyder, A. & Bisgin, H. (eds) Social, Cultural, and Behavioral Modeling. SBP-BRiMS 2018. Lecture Notes in Computer Science, vol 10899. Springer, Cham. https://doi.org/10.1007/978-3-319-93372-6_44

[3] Rege, A., Singer, B., Masceri, N. & Heath, Q. (2017). Measuring cyber intrusion chains, adaptive adversarial behavior, and group dynamics. 12th International Conference on Cyber Warfare and Security, 285-294.

[4] Rege, A., Adams, J., Parker, E., Singer, B., Masceri, N. & Pandit, R. (2017). Using cyber-security exercises to study adversarial intrusion chains, decision-making, and group dynamics. Proceedings of the 16th European Conference on Cyber Warfare and Security, 351-360.

[5] Arrow, H., & Crosson, S. (2003). Musical Chairs: Membership Dynamics in Self-Organized Group Formation. *Small Group Research*, 34(5), 523-556. https://doi.org/10.1177/1046496403254585

[6] Broadhurst, R., Grabosky, P., Alazab, & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. International Journal of Cyber Criminology. 8. 1-20.

[7] Nurse, J. and Bada, M. (2018). The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations. 10.1093/oxfordhb/9780198812746.013.36.

[8] Rege, A. (2009) What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. International Journal of Cyber Criminology. 3(2): 494-512.

[9] Rege, A., & Bleiman, R., (2020). Ransomware attacks against critical infrastructure. Proceedings of the 19th European Conference on Cyber Warfare and Security.

[10] Koppenjan, J. & Klijn, E. (2004). Managing Uncertainties in Networks, Routledge, London.

[11] Bennet, P., Cropper, S. & Huxman, C. (1989). Modeling interactive decisions: they hypergame approach, in Rosenhead, J. (Ed.), Rational Analysis for a Problematic World: Problem Structuring Methods for Complexity, Uncertainty, and Conflict, Wiley, Chichester.

[12] de Bruijn, H. (2005). Roles for unilateral action in networks. The International Journal of Public Sector Management, 18(4), 318-329. http://dx.doi.org.libproxy.temple.edu/10.1108/09513550510599247

[13] Rege, A., & Adams, J. (2019). *The need for more sophisticated cyber-physical systems war gaming exercises*. Reading: Academic Conferences International Limited. Retrieved from http://libproxy.temple.edu/login?url=https://www-proquest-com.libproxy.temple.edu/conference-papers-proceedings/need-more-sophisticated-cyber-physical-systems/docview/2261030019/se-2?accountid=14270

[14] McMullan, J. & Rege, A. (2010). Online crime and Internet gambling. Journal of Gambling Issues. 24. 10.4309/jgi.2010.24.5.

[15] Halvoresen, K.E. (2001). Assessing public participation techniques for comfort, convenience, satisfaction, and deliberation. *Environmental Management, 28*(2): 179-186. https://link-springer-com.libproxy.temple.edu/content/pdf/10.1007/s002670010216.pdf

[16] Cornish, D. & Clarke, R. (2008). The Rational Choice Perspective. In R. Wortley & L. Mazerolle. (Eds.), Environmental Criminology and Crime Analysis (pp. 21-47). Oregon: Willan Publishing.

[17] Clarke, R. & Felson, M. (2008). Introduction: Criminology, Routine Activity, and Rational Choice. In R. Clarke & M. Felson. (Eds.), *Advances in Criminological Theory, Volume 5* (pp. 1-14) NJ: Transaction Publishers.

[18] Campitelli, G., & Gobet, F. (2010). Herbert Simon's Decision-Making Approach: Investigation of Cognitive Processes in Experts. Review of General Psychology, 14(4), 354–364. https://doi.org/10.1037/a0021256

[19] GlobalCPTC. (n.d.) Retrieved January, from https://globalcptc.org/

[20] Holt, T.J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant behavior, 28(2),* 171-198.

[21] Hutchings, A. (2013). Hacking and fraud qualitative analysis of online offending and victimization. *Global Criminology: Crime and Victimization in a Globalized Era,* 93-112.

[22] Rege, A. (2016). Not biting the dust: using a tripartite model of organized crime to examine India's Sand Mafia. *International Journal of Comparative and Applied Criminal Justice, 40(2),* 101-121.

[23] Bachman, R., & Schutt, R. (2017). Fundamentals of Research in Criminology and Criminal Justice (4th ed.). Sage Publications.

[24] Buldas, A., Laud, P., Priisalu, J., Saarepera, M., & Willemson, J. (2006). Rational Choice of Security Measures Via Multi-parameter Attack Trees. 4347. 235-248. 10.1007/11962977