# The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations

Jason R. C. Nurse[1*] and Maria Bada[2]

[1] University of Kent, UK

[2] University of Oxford, UK

*j.r.c.nurse@kent.ac.uk

**Abstract**

While cybercrime can often be an individual activity pursued by lone hackers, it has increasingly grown into a group activity, with networks across the world. This chapter critically examines the group element of cybercrime from several perspectives. It identifies the platforms that online groups—cybercriminal and otherwise—use to interact, and considers groups as both perpetrators and victims of cybercrime. A key novelty is the discovery of new types of online groups whose collective actions border on criminality. The chapter also analyzes how online cybercrime groups form, organize, and operate. It explores issues such as trust, motives, and means, and draws on several poignant examples, from Anonymous to LulzSec, to illustrate the arguments.

**Keywords**

cybercrime, cybercriminal networks, organized crime, group behavior, human psychology, trust, criminal platforms, criminology

# Introduction

There are various perspectives through which cybercrime and its association with online groups can be studied, e.g., the groups that are responsible for cyber-attacks and similar acts of online aggression or the groups of individuals that are targeted. Anonymous is one of the most well-known of the hacker groups and has been linked to numerous high-profile online attacks. These include cyber-attacks on the FBI, US Department of Justice, and US Copyright Office (Peckham, 2012), declarations of war on banks and stock exchange markets (Schwartz, 2016), and more recent calls to action against U.S. President Donald Trump (Griffin, 2017). Other popular cybercriminal groups are Lizard Squad, a group that forced the Sony's PlayStation Network offline and caused a flight disruption with a bomb scare (Zorabedian, 2014); and the hacker group, Lulzsec, which stole private data from 24.6 million customers via a hack on Sony's PlayStation Network (Arthur, 2013).

In addition to these hacker groups, traditional organized crime groups are quickly expanding their presence into cyberspace. This is undoubtedly linked to the low barriers of entry, opportunity to vastly expand operations, and the perceived anonymity that the Internet provides. There is also a range of ad hoc groups consisting of members of the public who form online in support of a cause, but whose actions may be regarded as potentially criminal, e.g., the recent call to protest against Trump's January 2017 inauguration with a distributed denial-of-service attack (DDoS) (Metzger, 2017). This protest campaign was publicized online and requested that the public flood the WhiteHouse.gov website with requests to "demonstrate the will of the American people." Though the protest was later canceled because of the potential legal ramifications, it demonstrates the power of group action online.

Research has studied cybercriminal groups to varying extents to better understand their motivations, how they form and organize, and their techniques of attack (Choo & Smith,

2008; Olson, 2013; McGuire, 2012). Traditional organized crime groups, for example, are often driven online by the ability to up-skill quickly (via purchasing cybercrime services and tools) and therefore, to launch high-tech crimes with limited understanding and expertise (European Union Agency for Law Enforcement Co-operation, 2014). Online hacker groups are particularly interesting because unlike traditional groups, they may typically have to self-organize, i.e., as there may not be an agreed leader of the group to direct and co-ordinate operations, the group itself is responsible for these activities. Moreover, their actions are often based on causes, some of which the public may consider to be noble, and thus socially acceptable—the launch of #OpISIS, a cyber-attack campaign against the ISIS terrorist network after the 2015 Paris attacks is one example. In this case, Anonymous even posted a video declaring (cyber) war on the Islamic State group—targeting their websites and social media accounts—in response to attacks such as the Charlie Hebdo massacre in Paris in January 2015 that killed twelve people.

Another perspective in the study of the group element of cybercrime is a focus on groups as the target of crimes. Young Internet users, for instance, are often studied as they represent a particularly vulnerable group online (Kowalski, Giumetti, Schroeder, & Lattanner, 2014). Religion, as one might imagine, is also a topic that has resulted in numerous crimes online, particularly harassment and hate speech. Race is another polarizing subject in online communities, with many online hate groups actively congregating to voice their opinions (Chau & Xu, 2007). Additionally, there are many other groups that are commonly targeted in cybercrimes, e.g., females, the disabled, and lesbian, gay, bisexual, and transgender (LGBT) individuals. Online harassment and threats are two of the common types of aggression against these groups (Lenhart, Ybarra, Zickuhr, & Price-Feeney, 2016).

Having introduced the ways in which to consider the group element to cybercrime, the body of this chapter seeks to critically examine it in further detail. First, it considers the

platforms that are used by online groups, including Internet forums and mobile apps. Next, it examines the types of groupings present, including their actions and the factors that motivate crimes and draws heavily on case study examples arising from literature and the news. Then it builds on this foundation to analyze how criminal groups form and operate. This discussion encompasses issues of trust, motives, and means. The aim is to make these discussions pragmatic and provide useful insight into the group component of cybercrime, and issues such as interaction within criminal communities.

# Cybercrime and Online Groups

## Platforms Used by Online Groups: A Brief Look

Online groups and communities—or simply, people who interact via virtual environments—have existed since the dawn of the Internet. The first widespread groupings could be found on platforms such as Internet Relay Chat (IRC) and in chat-rooms on the once thriving AOL service. Since then, groups have spread to various other online services including social media services such as MySpace, Bebo, and Hi5, over the years. More recent social networks, including Facebook, host a number of groups on a range of diverse topics. The group aspect of Facebook is actually one of its most popular offerings with in excess of 1 billion users, and in December 2016, more than 10 billion comments and 25 billion likes (Frier, 2017). Other networks, such as Twitter and Instagram allow groups to chat, but these are currently via direct messages as opposed to being more openly accessible (to join, use, etc.), as with Facebook. We do note here however, that Facebook does have several closed groups where access is strictly moderated, and may be based on demographics, interest, status, or employer.

Research has explored groups' use of social media and, as alluded to above, they range from the benign to the more disruptive. For instance, groups have been used for teaching and improving writing (Yunus & Salehi, 2012), but also for activist networks, be they associated with contemporary activism or collective action (Gerbaudo, 2012; Vromen, Xenos, & Loader, 2015). One significant challenge for social network platforms in this context has been maintaining the balance between freedom of speech (or excessive censorship) and the public good, particularly when considering those activist groups that may be viewed as extreme. This is a problem that social networks have struggled with for many years, and one that does not appear to be solvable through any simple or individual means.

Forums are another popular venue where groups form and interact. This platform functions analogous to a message board with posts sequentially added by date and/or time to a webpage. Some of the most well-known forums online are Reddit (the self-deemed "Front page of the Internet"), CraigsList (a classified advertisements and discussion website), and 4Chan (an image-board website that allows anonymous posting). Positive uses of forums can be seen in activities such as support groups and those used for health advice (Cole, Watkins, & Kleine, 2016), though negative uses are also abundant. Articles in research have even emphasized that Internet forums often act as an efficient and widely used tool for radical, extremist, and other ideologically "sensitive" groups and organizations to connect and inform on their agendas (Holtz, Kronberger, & Wagner, 2012).

While cybercriminal and terrorist forums can be found on the open web, the most significant and devious are rife on the Dark Web. The Dark Web is the part of the web which exists on an encrypted network and can only be accessed using specific software and networks, such as Tor (or, The Onion Router) and I2P (the Invisible Internet Project). These services provide some level of anonymity hence their attraction to criminals. Dark Web

forums and communications have been the focus of researchers for several years as they attempt to better understand how cybercriminals behave and act (TrendMicro Inc., 2016).

To complement online social media and forums, there are an increasing range of applications which allow groups to form and communicate. WhatsApp is one of the most popular of these applications, with around 1 billion users. This platform allows individual and group chat, and boasts secure messaging, a feature which has privacy advantages but is also heavily contested by governments and intelligence communities. Secure messaging in this context refers to WhatsApp's use of full end-to-end encryption, which means that the only persons who can read messages (including photos, videos, files, etc.) are the sender and the intended recipients. As pointed out by WhatsApp, even they cannot see inside the messages (WhatsApp, 2017).

A key reason why there is such heated deliberation around the services of WhatsApp and Telegram (a service similar to WhatsApp which also has end-to-end encrypted messaging), is because they may be seen as a safe space for terrorists and other criminals (Magdy, 2016). There is no shortage of news articles and blogs which suggest this, as can be seen from the following story titles: "Paris terrorists used WhatsApp and Telegram to plot attacks according to investigators" (Billington, 2015), "Inside the app that's become ISIS' biggest propaganda machine" (Engle, 2015), "How Telegram Became The App Of Choice For ISIS" (Robins-Early, 2017), "How terrorists use encrypted messaging apps to plot, recruit and attack" (Hamill, 2017), "WhatsApp accused of giving terrorists 'a secret place to hide' as it refuses to hand over London attacker's messages" (The Rayner, 2017) and "Indian Govt May Ban WhatsApp Use In Country, As It Is Terrorist's Favourite App For Messaging" (D'Mello, 2018).

Other apps and instant messaging services that authors (e.g., Magdy, 2016) have found that may be used by activist groups include WeChat (a China-based platform that has over 1

billion monthly active users), SureSpot (an open-source secure mobile messaging app that uses end-to-end encryption) and Kik (a messaging platform originating in Canada that has approximately 300 million users). To add to these, a topical study by TrendMicro of over 2,000 accounts that openly support terrorist groups has also found Wickr (an app that offers secure, ephemeral messaging) and Signal (an open source encrypted communications app) as preferred apps for these groups of individuals (TrendMicro Inc., 2016). As noted by Magdy (2016), this range of apps may be used for different purposes but generally their popularity is driven by the fact that they allow faster, more personalized and secure communication.

## Groups as Perpetrators and Victims of Cybercrime

The platforms presented above have supported a range of activities pertaining to the group element of cybercrime. As discussed earlier, at least two approaches that could be explored are groups as the perpetrators and initiators of crime, or groups as the victims thereof, for instance, targeted demographics or minorities. Our aim in this section is to reflect on the group element of cybercrime more critically and identify the set of core group types. These would be beneficial to research and practice in the fields of study in cybercrime, cyberpsychology and criminology.

We begin this analysis with a consideration of the perpetrator's perspective and thus, first look to understand how the public and literature perceive criminal groups. The three descriptions of criminal groupings that form the basis for our discussion are taken from the US Federal Bureau of Investigation, and the research works of Finckenauer and Voronin (2001) and Godson (2003). We focus on organized criminal groups here as these are the most commonly discussed in the literature.

The US Federal Bureau of Investigation (FBI) considers the topic of transnational organized crime and the definition they ascribe to is:

> "Those self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, and monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms." (FBI, 2016)

From an academic perspective, Finckenauer and Voronin give insight into the group nature of crime through their definition of organized crime.

> "Organized crime is crime committed by criminal organizations whose existence has continuity over time and across crimes, and that use systematic violence and corruption to facilitate their criminal activities. These criminal organizations have varying capacities to inflict economic, physical, psychological, and societal harm. The greater their capacity to harm, the greater the danger they pose to society." (Finckenauer and Voronin, 2001, p. 2)

Finally, Godson provides another academic definition on organized crime as he notes:

> "Organized crime refers to individuals and groups with ongoing working relationships who make their living primarily through activities that one or more states deem illegal and criminal. Organized crime can take a variety of institutional or organizational forms. This includes tight vertical hierarchies with lifelong commitments, as well as looser, more ephemeral, nonhierarchical relationships." (Godson, 2003, p. 274)

Reflecting on these three definitions, we can begin to see some of the key features of criminal groups. For instance, there is the notion of continuity and group identity in the group (and

member relationships) and criminal activities over time. This is particularly evident in the descriptions from the FBI and Finckenauer and Voronin. Motivation is another feature that stands out in the definitions, with influence and financial and commercial gain, acting as common reasons for group formation and crimes. Finckenauer and Voronin extend this point to highlight the generic aims of crimes; that is, inflicting economic, physical, psychological, and societal harms, but also the varying capabilities that criminal groups may possess in achieving such goals.

Godson touches on another important feature in terms of the various organizational forms that groups may take; for instance, they may be tightly bound or ephemeral and non-hierarchical. Group shape will likely depend on their nature and purpose, and the extent to which their activities will interest law enforcement. The FBI description is useful particularly because it emphasizes the transnational nature of criminal groups and their use of global communication channels, many similar to the platforms discussed earlier in this chapter and other chapters (see Nurse, this volume).

The reflection on criminal groups is crucial to the discussion on cybercrime for numerous reasons. In particular, there is almost certain to be many similarities between these groups considering that the Internet may be regarded as just another platform through which crime can occur. The various descriptions above can all be related in some way to cybercriminal groups. The main difference with cybercriminal groups is their focus on technology as a central means for interaction and criminal acts. Unlike traditional crime therefore, physical presence and power (including physical violence) is not as crucial, and technical means and skill tend to be more important. Furthermore, because of technology, cybercriminal groups can become transnational much more easily as they can meet and interact via the various platforms mentioned. Such interactions may be persistent or temporal depending on the nature of the crime. As we will discuss later, there is also the reality that

with the Internet, forming groups of like-minded individuals is significantly easier than it is offline. There is less risk to group formation and persistence as well, given the ability online to mask one's identity—these factors often combine to the advantage of criminals. Technology also means a wider availability of hacking platforms and tools, a reality that is predicted to increase in the future via a proliferation offensive tools (Williams, Axon, Nurse et al., 2016).

Cybercrime groups have been of interest to researchers for some time, and therefore it is not surprising that articles have proposed ways to typify such groups. Possibly one of the most notable pieces of research on the topic is by Choo and Smith (2008). They explore the exploitation of online systems by criminal groups and have defined three categories of such groups. The first category is that of traditional organized criminals who use technology to enhance terrestrial criminal activities. This includes crime syndicates and organized groups that specialize in everything from fraud and forgery to piracy and extortion from online gambling. Their aim is often to apply technology to expand and streamline operations.

Europol has carried out extensive work in the cybercrime space and have highlighted the prevalence of crime-as-a-service business models as a facilitator for traditional groups engaging in cybercrimes (European Union Agency for Law Enforcement Co-operation, 2014). Crime-as-a-service models, which can typically be found on underground Dark Web markets, allow criminals to purchase criminal services including acquiring botnets (or spam networks), launching denial-of-service attacks against specified targets, and customized malware development. As such, criminals can easily and quickly launch sophisticated cyber-attacks on groups or individuals of their choosing.

Organized cybercriminal groups are the second category identified by Choo and Smith and are said to be groups comprised of like-minded individuals working collectively towards a common goal. The Internet is a central enabler to such groups as it is the platform that they

meet and plan activities; furthermore, their members may only be known to each other online. These are a few of the factors that distinguish these groups from traditional organized criminals which use technology to enable crimes. One example of such a group is the hacking group Lulzsec, where there are reports that their members never met in person, and were unaware of each other's identities (Arthur, 2013). Another recent example is the Carbanak cybercrime group, named after a piece of malware it used to access banking systems. The head of this group was the mastermind, and also technically talented enough to be able to identify software vulnerabilities and write malware to exploit them (Burgess, 2018). According to reports, the head of the group also worked with three other gang members, who did not know each other and instead chatted online (Burgess, 2018).

The last group category is that of ideologically and politically motivated cyber groups. This spans terrorist organizations and the full range of hacktivist groups. Choo and Smith make an intriguing point in their characterization of this category of groups. That is, that crimes often associated with organized criminal groups (e.g., scam and fraud schemes) are also crimes which terrorist groups engage in to raise funds for their ideological pursuits. A 2015 U.K. report showed that scamming and ransoms are high on the list of activities undertaken for terrorist financing (HM Treasury and Home Office, 2015). Terrorist groups, e.g., ISIS, are widely known to engage in online activities, but particularly for plotting, recruiting, and claiming responsibility for attacks (Engle, 2015; Nouh, Nurse, & Goldsmith, 2016; Hamill, 2017). Social media continues to be a favored platform for such groups, e.g., the role of Twitter in "Tweeting the Jihad" (Klausen, 2015).

Hacktivists, or politically-motivated hackers, are also an increasingly popular grouping in this cybercriminal category. Such groups are known to carry out activities against governments and large corporations. Anonymous is one of the most well-known of these groups, given its attacks on the FBI and other sites (Peckham, 2012). A key factor that makes

Anonymous stand out potentially even more however, is its public-facing nature. There have been a variety of books published on Anonymous including Parmy Olson's We are Anonymous (2012) and Gabriella Coleman's Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous by (2014). Moreover, documentaries have been released on the workings and beliefs of its members—see We Are Legion: The Story of the Hacktivists (2012).

Anonymous also maintains a significant presence on social media. At the time of writing, for instance, they appear to possess several Twitter profiles including @AnonyOps, @YourAnonNews, @YourAnonGlobal, @GroupAnon, @AnonPress, and @AnonyPress; the most popular being @YourAnonNews with more than 1.6 million followers. These various accounts hint to a core value of Anonymous, namely, the lack of central or hierarchical structure (as will be discussed in the third section of this chapter). This is clearly exemplified in the @GroupAnon tweet: "No, this is not the official #Anonymous account. There is no official account. We have no central leadership. (Other than the FBI/NSA, joke)" made on 10:39 a.m. 18 Nov 2015.

While the three main groupings highlighted here are undoubtedly the core criminal networks, the authors of this chapter believe that there is another group, whose criminality is much more subjective, emerging in society today—individuals (often not criminals) who use technological means to motivate and organize acts that may be deemed dangerous or illegal. In Section 1, we presented one of these cases where there was a call to protest against President Trump's January 2017 inauguration using a distributed denial-of-service attack (DDoS) on WhiteHouse.gov (Metzger, 2017). DDoS are regarded as criminal acts by many given that they are commonly used by hacker collectives to force legitimate websites offline.

The case of President Trump is interesting for many reasons. For example, there have been many rallies and protests against President Trump since he began his election campaign,

several of which were organized online (CBS News, 2017). While participating in rallies and protests is every citizen's right, the challenge of crime arises when these protests turn violent as they did in Portland, Oregon after the election and in Washington DC at the time of President Trump's inauguration. In DC in particular, demonstrators set cars on fire and smashed shop and car windows (Longbottom, 2017).

Civil action, organized via online networks and platforms, has also been witnessed in many other parts of the world prior to these U.S. instances. In the UK in 2011, thousands rioted following the death of local man Mark Duggan who was shot by the police; these riots led to mass looting and millions of pounds worth of property damage. It is said that the Blackberry Messenger app played a crucial role in the organizing the riots (Fuchs, 2012) in enabling contagion and a group-mob mentality; Reicher (2001) and Stott, Drury and Reicher (2016) provide further insight into the psychology of crowd dynamics broadly, and in the London riots, respectively. Facebook has also been used by activists as a platform for action and engagement with increased online activity found to often correlate with offline group actions (Nouh & Nurse, 2015). In 2010's Arab Spring, Facebook was used to spread the word of the revolution, and many believe that social media contributed to the liberation of those societies (Fuchs, 2012). These are all instances where technology and online interactions have contributed to offline unrest (be it positively or negatively motivated) and, in some instances, crime. There are many group processes at play in these instances, as there are offline. Establishing group identity and common goals plays a crucial role in bringing together individuals to create these groups.

In addition to the work by Choo and Smith (2008), other articles that have sought to identify the types of cybercriminal group include McGuire (2012) and Leukfeldt, Kleemans, and Stol (2016). McGuire suggests a typology of cybercrime groups with three main types. These are, groups that operate primarily online, those that combine online and offline

activities, and groups that are predominantly offline but use online technologies as an enabler for crimes. This typology therefore closely matches up with the categorization of Choo and Smith. The research by Leukfeldt and colleagues adds another dimension to the analysis of cybercrime groups by considering them according to their characteristics. Specifically, they propose technology use (low-tech to high-tech) and the level of offender-victim interaction (no interaction to high interaction), while also noting the extent to which groups have local or international components. The benefit of such an approach is that it allows the correlation of characteristics, and in their case, the discovery of which types of network operate at which levels.

Having reflected on the perpetrator perspective of cybercrime and groups, we now consider the viewpoint of groups as the victims of online crime. While practically any demographic or characteristic can be used to target groups of individuals, some of the most common are those of race, religion, age, gender, and sexual-orientation. It is worth noting that these characteristics are not specially targeted in the online space but happen to be more openly targeted because of the illusion of attacker anonymity online. There are plenty of examples of groups that have formed online to preach hate towards persons of the characteristics highlighted. Chau and Xu (2007) study one such type of hate group of "anti-Blacks" covering 820 bloggers on blog-hosting website, Xanga. A key finding from that research is that hate groups in the blogosphere may not tend to form into centralized organizations. The authors, however, do not eliminate the possibility that such online groups may prepare members for other extremist organizations such as the Ku Klux Klan, for instance.

Beyond race, religion is a significant factor in online victimization. A salient example of this victimization occurred after the Woolwich attack in May 2013 in the UK, where two Islamist terrorists brutally murdered a British soldier. In the days that followed, there were

hundreds of messages on social networks containing hate speech directed against the Muslim community (Awan, 2014). Awan found that Muslims were demonized and vilified through negative comments, discrimination, physical threats, and online harassment. Other works have demonstrated this hate towards groups in online message boards as yet another example of how online platforms can be used to target people of certain faiths (Cleland, Anderson, & Aldridge-Deacon, 2017).

While other groups (females, the disabled, and lesbian, gay, bisexual, and transgender (LGBT) individuals) are also the victim of online harassment (Lenhart et al., 2016; Chahal, 2016), youth are a particularly well considered area (by both academia and law enforcement) given their vulnerable nature. Kowalski and colleagues (2014) focus on the crime of cyberbullying among young people to provide a critical review of the existing body of cyberbullying research. Mitchell, Wolak, and Finkelhor (2008) also offer relevant insight that young Internet bloggers also were at an increased risk for online harassment. Furthermore, young individuals who interacted with people that they met online were at a higher likelihood of receiving online sexual solicitations. Population-based studies from other countries, e.g., Oksanen and Keipi (2013), have supported these points and found that young people are generally more likely to be victims of cybercrime. A key novelty of their work is that they consider the risks of victimization that young people face online, to the problems they may face in the offline world.

Drawing on this analysis of the group component of cybercrime,

Table 1 presents two main group types of groups: perpetrators and victims of criminal acts. The core subtypes of the former group are largely motivated by the work of Choo and Smith (2008). To this has been added a new group focusing on citizens who use online technological means to mobilize and act. It is important to note that, in most instances, such action is not criminal and only in a few cases results in criminal acts (e.g., offline riots or

looting). Furthermore, there may be arguments that this group is already accounted for in the "Organized ideologically and politically motivated cyber groups." It is presented separately here due to its increasing importance in society (with the Arab Spring and the Trump protests arguably only the beginning of what is to come) and the difficulty in categorizing it, given it often borders on criminality.

**[Insert Table 1 here]**

With regards to the category of groups as victims, the subtypes listed have been studied in various articles before. The list included in Table 1 is based heavily on such works and instances of discrimination, victimization, and harassment found online. It is worth noting that these groups align broadly with the protected characteristics of the UK's Equality Act 2010 and similar legislation across the word. This emphasizes their significance in society more widely other than just in cyberspace. Over the next few years, there is expected to be a sharp growth in research into "groups as victims" online, particularly because of the difficulty that platforms such as Facebook and Twitter have in detecting and responding to online abuse and harassment.

# How Online Criminal Groups Form and Operate

With the main types of groups identified, this section narrows the focus to "groups as perpetrators." It concentrates specifically on how cybercriminal groups form, engage, and operate.

## Group Formation and the Platforms and Networks That Enable It

Case studies suggest that within cybercriminal networks the importance of traditional central actors with the role of "bridge builder" diminishes (Holt & Smirnova, 2014; Motoyama,

McCoy, Levchenko, Savage, & Voelker, 2013). However, recent studies also show that such networks still have important social dependency relationships (Leukfeldt, Kleemans, & Stol, 2016, 2017; Leukfeldt, de Poot, Verhoeven, & Lavorgna, 2017). Research demonstrates that most of the networks have a (more or less) stable group of core members who commit crimes together over an extended period of time. The core members of these networks may know each other from the offline world and recruit only a few specialists through online meeting places. Other studies suggest that cybercriminal networks use offline social ties and, on occasion, online meeting places to come into contact with suitable co-offenders (Leukfeldt, Kleemans et al., 2016, 2017; Odinot, Verhoeven, Pool, & De Poot, 2016). Thus, the reality is that a minority of networks could be labeled as ad hoc networks that were forged in online meeting places to execute one-off cyber-attacks.

Social ties may be strongly clustered and limited to, for example, a region or country. Members of some cybercriminal networks are located in the same offline social cluster—even when executing cybercriminal attacks all over the world (Leukfeldt, Kleemans et al., 2016, 2017; Odinot et al., 2016). Working with trusted acquaintances from the offline world could potentially have many advantages over working with potentially unreliable actors from all over the world who are only known by their online handle (pseudonym).

As with most situations, there are some exceptions to the common case where offenders are distributed across the Internet and not necessarily geographically located in one single place. The hacking group LulzSec is an example of this which is held to have been formed in private online chatrooms of the hacking collective Anonymous. Most notably, LulzSec members never met in the real world (Arthur, 2013). From this example, it can be inferred that cybercrimes and cybercriminals, by their very informational, networked, and global nature, may go against the traditional model of socially and geographically rooted organized crime models. This pertains to the need to gather specialist skills; in particular, such groups

tend to have a very detailed division of labor with specific skill sets across individuals. For instance, one person would provide the documents, another would buy credit card details, still another would create identities, and a fourth would provide the drop address (Rodgers, 2007).

Furthermore, not all cybercriminals commit only cybercrimes. Studies suggest that cybercriminals are often also involved in all sorts of offline crimes (Leukfeldt, Kleemans et al., 2016; Van Der Broek, Van der Laan, & Weijters, 2016). Yet, in the online world, distance, location, and time are no longer limiting factors. Compared to the offline world, it is relatively easy for offenders to be part of different criminal networks. For example, newcomers on forums are able to come into contact with existing members quickly and are able to reach a more central position relatively quickly.

To consider enabling platforms for criminal activities, the Internet has several criminal meeting places. Two examples are the forums and chat rooms where criminals meet to exchange information or make plans to carry out attacks. To a certain extent, forums can be regarded as platforms that facilitate the origin and growth of cybercriminal networks. Members of cybercriminal networks spend much of their time in criminal and non-criminal chat rooms and forums, where they meet like-minded people and build relationships. As mentioned, existing offline cultures, communities and social relationships also appear to be important in online forums (Ablon, Libicki, & Golay, 2014).

Additionally, Leukfeldt, Kleemans et al. (2016) found that both social ties and online forums were used by cybercriminal networks to recruit new members. Four types of growth were identified in their work: 1) growth entirely through social contacts; 2) social contacts as a base and forums to recruit specialists; 3) forums as a base and social contacts to recruit local criminals; and 4) growth entirely through forums. Criminals would usually recruit through social ties and less through social contacts and use forums in order to find specialized enablers. An example of such a group is LulzSec. LulzSec's members never met in the real

world and were unaware of each other's identities. Some were based in the US, and some in the UK, demonstrating the globalized nature of such groups.

Cybercriminals show a noticeable preference for carding forums. These are websites dedicated to the sharing of stolen credit card information as well as providing discussion boards in which members of the forum may share techniques used in obtaining credit card information. Using interaction data from three prominent carding forums—Shadowcrew, Cardersmarket, and Darkmarket—and drawing on theories from criminology, social psychology, economics, and network science, Yip, Webber, and Shadbolt (2013) identified fundamental socio-economic mechanisms offered by carding forums: formal control and co-ordination, social networking, identity uncertainty mitigation, and quality uncertainty mitigation. Together, these mechanisms give rise to a sophisticated underground market regulatory system that facilitates underground trading over the Internet and thus drives the expansion of the underground crime economy. This demonstrates the robustness of carding forums and alludes to why they are favored by cybercriminals. Moreover, Holt and Lampke (2010) manually analyzed six forums and found that the dynamics of the stolen data markets are governed by key factors, including communications, price, quality, and service. This is intriguingly similar to legitimate markets.

To understand the cyber-threat landscape, it is also important to acknowledge the different ways that cybercriminal groups are organized. First, the cybercrime-as-a-service business model that drives criminal forums on the Dark Web provides the access to tools and services to people with little knowledge of cyber matters. Furthermore, the environment promotes exchange of information as well as "learning kits." This trend is indicative of a growing cyber capability among these criminal groups as their knowledge expands and they exchange expertise. As some terrorist groups are reaching out to recruit in the Western world, they might be able to contact and attract appropriately skilled people for their hacking

exploits (European Union Agency for Law Enforcement Co-operation, 2014; National Cyber Security Centre, 2017).

For the most organized and technically advanced groups, however, many of the services are carried out "in-house" as part of their own business model. For smaller groups or individual criminals, these services can be hired in one of many online criminal marketplaces. Most of these services like crime-as-a-service are openly advertised in criminal forums. As Richardson (2007) states, hackers have organized and shifted toward a "professionalization" of computer crimes. A few examples of such criminal forums are Dark Market, Carders Market, Shadowcrew, Carder.su, Darkode, GhostMarket, and the Silk Road.

To analyze the relationships among hackers more generally, it is often common to find a decentralized network structure. Network centralization describes a quality of a group and it indicates the extent to which a network is organized around one or more central points, such as a node or a centroid (Wasserman & Faust, 1994; Nouh & Nurse, 2015). Previous research has shown that the Shadowcrew hackers, for example, were part of a decentralized network, although not everyone in this group had the same type of role or position (Lu, Luo, Polgar, & Cao, 2010). The network structure of this infamous hacker group was established using social network analysis methods. Leaders were identified using actor centrality measures (degree, betweenness, closeness, and eigenvector) and were found to be even more involved in thirteen smaller sub-groups (Lu et al., 2010). Shadowcrew had the three characteristics of a team as defined by Best and Luckenbill (1994): 1) elaborate division of labor; 2) mutual participation; and 3) association. From this observation, the inference is that the members of cybercriminal groups do not necessarily have to be organized around one central point in order to still maintain a hierarchical structure.

In addition, the organization of crime online may often follow a different logic to the organization of crime offline. This is a dis-organized model of organization (Wall, 2007).

Existing work identifies a "dis-organized" or distributed model of organization, rather than a hierarchical command and control structure of cybercrime (Wall, 2015). Network technologies and associated social media are creating new forms of networked social relationships that act as the source of new criminal opportunities (Wall, 2007) and crimes such as stalking, bullying, fraud, and sextortion.

Anonymous is an example of a group which does not strictly organize itself and has both swarm and hub characteristics. The fact that Anonymous has no leader makes it difficult to even comprehend its organizational structure (Norton, 2012). The structure of Anonymous has been loosely described as "a series of relationships" with no membership fee or initiation. Anyone who wants to be a part of Anonymous—an Anon—can simply claim allegiance. Many Anonymous members considered themselves crusaders for justice. Publicly, Anonymous persists in claiming to be non-hierarchical (Kushner, 2014).

Apart from collaborating and recruiting their members, it is also interesting to note that organizations operating on the Dark Web seem to also be attacking each other, and trying to prevail over their criminal competitors (Catakoglu, Balduzzi, & Balzarotti, 2017). These attacks could be defacements aimed at subverting the business of another organization in order to promote a competitor website; attempts to spy on communications initiated to, and from, another organization, theft of confidential data from a disguised File Transfer Protocol (FTP) server, or manual attacks against the custom application running the underground forum. These activities demonstrate the tensions between groups as they participate in these various platforms and networks.

## Trust as a Factor for Cybercriminal Group Formation

The concept of trust within the human factors domain has focused largely on the user gaining trust as a result of specific website content, attributes, ease of use, and related consumer-

centric acceptance models (Corritore, Kracher, & Wiedenbeck, 2003; Nurse, Rahman, Creese, Goldsmith, & Lamberts, 2011). Trust is an enabler of online engagement but also certain levels of trust are required when assessing what is being offered or accessed.

Supporting the growth of the Dark Web, and presumably the trust gained by participants to engage, are anonymity networks like Tor. In fact, it is a mandatory feature of a number of Dark Web forums that participants use Tor and agree to transact only through the use of virtual currencies, such as Bitcoin (Bradbury, 2014) and, increasingly, Monero (a virtual currency with a strong focus on privacy). The users of cybercrime marketplaces must trust that such environments will maintain their anonymity and will also follow through with the service communicated, e.g., provision of information on stolen credit cards. Ironically, the uniqueness of the trust environment for Dark Web participants and hosts appears to distil to the singular issue of preserving anonymity (Lacey & Salmon, 2015). Integrity as a basis for trust in the Dark Web can encapsulate the overall integrity of the marketplace in maintaining anonymity of its users and hosts, which also connects to Mayer, Davis and Schoorman (1995), who observed that anonymity is a binding mutual interest for participants. Trust is dynamic, because it can build, diminish, and be removed at any point.

According to Falcone, Singh, and Tan (2001), various different kinds of trust should be modeled, designed, and implemented when speaking about trust in cyber-societies: 1) trust in the environment and in the infrastructure (the socio-technical system); 2) trust in personal agents and in mediating agents; 3) trust in potential partners; 4) trust in information sources; and 5) trust in warrantors and authorities. Parts of these different kinds of trust have complementary relations with each other. The final kind—trust in a system and/or process—can be the result of various trust attributions to the different components. When an agent has to decide about whether to trust another agent in the perspective of a co-operative relationship, each must weigh the opportunities given by the positive results of a successful

trust (benefits of trust) against the risks that the trust might be exploited and betrayed: this problem is known as the trust dilemma. The trust dilemma is the direct consequence of uncertainty—here, the intrinsic social uncertainty (Falcone, Singh, & Tan, 2001), and is similar to the social exchange principle engage in offline relationships to garner trust between one or more people (Thibaut & Kelley, 1959).

For all criminals, a balance must be made between remaining anonymous in order to remain unseen by law enforcement, and retaining certain aspects of identity in order to attract potential criminal collaborators (Lusthaus, 2012). Online identities are the foundation of a cybercriminal's reputation, which provides incentive to maintain that identity or a variation of it. At the same time, there is a competing incentive to change online names regularly in order to create a distance from past crimes. Reputation in some ways may be regarded as the "currency" that cybercriminals trade in on the Dark Web.

Gambetta's (2009) contributions to both criminology and signaling theory expand the understanding of the ways criminals identify themselves to each other and signal trustworthiness in an otherwise untrustworthy environment. Specifically, when there is information asymmetry, it is in a signaler's best interests to signal their trustworthiness, regardless of whether they actually are. Untrustworthy actors attempt to mimic the signals used by their trustworthy counterparts, and it is in the receiver's best interest to differentiate between the two. Legitimate actors use signals that may be too costly for untrustworthy actors to replicate, which provides a potential way for receivers to interpret signals produced. To minimize the risk of harm, forums provide informal mechanisms that encourage trust between participants and sanction less reputable actors (Holt, Smirnova, Chua, & Copes, 2015). Other options also include having required reputation or history to enter closed online forums or to earn the status of "trusted seller" (Yip, Webber & Shadbolt, 2013; Yip, Shadbolt, & Webber, 2013).

Even with a system such as a carding forum that is capable of providing multiple channels for trust to develop, there is still room for mistrust (McCarthy & Hagan, 2001; Chiles & McMackin, 1996). In cases of mistrust, members of groups can be doxxed, such as the true identities of the members of the LulzSec gang that were made public, which ultimately led to the FBI arresting LulzSec leader Hector "Sabu" Monsegur (Bright, 2012). The interested reader is referred to the previous chapter for further information on doxxing and other common cybercrimes (see Nurse, this volume).

The Darkode forum, which had between 250–300 members, is another interesting case that operated very carefully and was very exclusive. Darkode administrators made sure prospective members were heavily vetted (FBI, 2015). Similar to practices used by the Mafia, a potential candidate for forum membership had to be sponsored by an existing member and sent a formal invitation to join. In response, the candidate had to post an online introduction—a resume—highlighting their past criminal activity, particular cyber skills, and potential contributions to the forum. The forum's active members decided whether to approve applications, which showcases the importance of trust in the formation of cybercriminal groups.

## Group Operations, Their Motives and Means

Different organizations such as Anonymous, LulzSec, and the Ghost Security Group each illustrate quite different sets of offender motivations, levels of professionalism, and organization, but they also possess some similarities in terms of their organizing principles (Wall, 2015). There may even be noteworthy patterns and motives across the groups linked to the motive, operating capability and attacks of the cybercriminals (Thornton-Trump, 2018).

A core dynamic of different groups appears to be based upon a reputational economy that binds the group together. As Wall (2015) describes, when looking at the similarities of

different groups, it is possible to identify that the key players seek the assistance of a broader group of participants who exist outside the central grouping, but within the idea frame (the crime-motive). These can help in solving problems related to the criminal activity being designed, built, or carried out. There may even be a further layer of individuals linked to the group who are outside the idea frame and who will give advice on specific issues. Sometimes individuals fall out of the information loop, or they are pushed out, or they leave, which makes the structure ephemeral. In most cases, the structure of the group is flat and lacks a hierarchical command and control form.

In brief, cybercriminals display common characteristics in that they often are fairly ephemeral and amorphous in terms of organization, and flex according to the demands and opportunities. They also seem to be self-contained in structure (McGuire, 2012; Yip, Webber & Shadbolt, 2013). They may regularly be driven by an individual or by a very small group, but not always, because the organizing principle is often like-mindedness with a central common idea or ethic. In Anonymous, for instance, each cell or subgrouping follows an idea frame (motive). There are not necessarily any relationships or even communications between cells outside the nucleus, just an identification and affiliation with the core idea. The interesting fact here is that this distributed type of organization does possess some similarities with the organization of many offline organized groups. They also reflect the United Nations Office on Drugs and Crime (UNODC) (2002) organized crime group typologies.

One of the most interesting aspects of these communities is that of their characteristics and how they function. For instance, these individuals are likeminded and therefore have some shared culture, at least in the context of their actions. This culture includes values as well as intergroup dynamics. These include own-group perceptions, attitudes, and behaviors, as well as those towards another group. A cybercriminal's social identity may be defined by

group membership, as well as the general features that define the group and differentiate it from others (Hogg & Williams, 2000).

The most sophisticated cybercrime organizations are characterized by substantial functional specialization and divisions of labor (Broadhurst, Grabosky, Alazab, & Chon, 2014). The organization of cybercrime may also occur at a wider level and involve networks of individuals who meet and interact within online discussion forums and chat rooms. Some discussion forums function as "virtual" black markets that advertise, for example, stolen credit card numbers (Holt & Lampke, 2010). A comparison of individual offenders and criminal organizations reveals that both possess impressive skills (Broadhurst, Grabosky, Alazab, & Chon, 2014). Odinot and colleagues (2016) suggest the characteristics of offenders that are important in the offline world, such as age, physical health, and social behavior, are less important within cybercriminal networks. There are new types of offender not previously found among traditional organized criminal groups: those with an IT background, young offenders, and ill/disabled offenders.

Criminal organizations might also possess a variety of aims, including defiance of authority, freedom of information, sexual gratification of members, and technological challenge. However, the profit motive is more apparent in the organizational cases than with individual offenders, as are the activities undertaken by organizations operating under state auspices, specifically those involving espionage and offensive cyber operations.

While profiling cybercriminals of any type, there are specific common characteristics requiring investigation, such as technical know-how, personal traits, social characteristics, and motivating factors (Nurse et al., 2014). These have been derived from over 100 cases and exclusive reviews of pertinent literature regarding crimes. Often, the prime motivator for the majority of cybercriminals is not only easy profit, but also curiosity (Malenkovich, 2012). Furthermore, in evaluating the motivation of cybercriminals, it is safe to state that some

criminal action will be motivated by "need" (Maslow, 1954) or by work and/or environment characteristics (Hunt & Hill, 1969). For example, different groups such as Anonymous, LulzSec, and the Ghost Security Group each illustrate quite different sets of offender motivations, levels of professionalism, and organization, but they also possess some similarities in terms of their organizing principles (Wall, 2015).

In terms of motive, Shinder (2010) lists monetary gain, emotion, political or religious beliefs, sexual impulses, or even boredom or the desire for "a little fun." While these factors are obviously linked to traditional or real-world crime, what is not yet clear is whether cybercrime has the same associations or etiology. Critical in this regard is the understanding of motive: transition from initial motive to sustaining motive, overlapping motives, and the prediction of evolving motives, along with an understanding of primary and secondary gains.

For example, a hacker becoming part of a community of like-minded persons involves a subcultural aspect inherent within creating online relationships that allow a hacker to express themselves (Bossler & Burruss, 2010). This subculture might be characterized by the perception that committing cybercrimes is something normal. Within a group there will exist some resistance to perform immoral activities, while others with a lower moral threshold may opt or enlist to perform them to increase their benefit (Atkinson, 2015). It is of note that cybercriminals will protect the infrastructure rather than destroying it to keep making money from the persons and/or networks that they have compromised (Aiken & McMahon, 2014).

Perry & Olsson (2009) found that the Web created a new common space that fostered a "collective identity" for previously fractured hate groups, strengthening their domestic presence in counties such as the US, Germany, and Sweden. McDevitt, Levin, and Bennett (2002) identified broad categories of hate crime offenders: 1) thrill offenders—those who commit their crimes for the excitement or the thrill; 2) defensive offenders—those who view themselves as defending their "turf"; 3) mission offenders—those whose life's mission is to

clear the world of groups they consider evil or inferior; and 4) retaliatory offenders—those who engage in retaliatory violence. Therefore, the motives of these groups define the way they operate.

Models of small group dynamics suggest how conformism, the influence of extremist ideologies on moving people to more extreme attitudes, disinhibition, and the yearning for group acceptance can all conspire to drive a person to commit acts of hate crime (Rieker, 1997). Hate crimes can also be committed due to psychological, social-psychological, historical-cultural, sociological, economic, and political reasons (Green, McFalls, & Smith, 2001).

LulzSec, Anonymous, and the Ghost Security Group offer useful practical examples. In the case of the first, the intention appeared to be gaining attention, embarrassing website owners, and ridiculing security measures (Arthur, 2013). For Anonymous-affiliated activists, perhaps the highest profile was their work under the banner "Operation Isis," or #OpISIS, which consisted largely of finding Twitter feeds that supported the ISIS terrorist group (and were often used to distribute propaganda and share news releases) and reporting them to Twitter so that they could be shut down (Griffin, 2015). Lastly, Ghost Security Group also engaged in similar targeting of jihadists by monitoring suspected ISIS Twitter accounts and infiltrating militant message boards to find information, which they would then pass along to law enforcement (BBC, 2015). These actions could be considered noble and of benefit to society, therefore hinting at the varying motives and values of such groups.

However, there are several instances to the contrary, e.g., under the banner #OpTrump Anonymous targeted Donald Trump before he was elected president. The attack led to temporary shutdowns of Mr. Trump's website and alleged hacks of his voicemail (Griffin, 2017). It is worth reiterating that announcing that their next target would be the Trump campaign set off the most heated debate yet within the movement. Many disavowed the anti-

Trump operation as being counter to Anonymous' tradition of not taking sides in political contests (Woolf, 2016). These conflicting aims are not surprising, given the dispersed nature of this cybercrime group. More importantly, it provides a perfect illustration of the context and reality of such online criminal groups and generally issues related to the group element of cybercrime.

# Conclusion

This chapter reflected on the group element of cybercrime to develop a better understanding of how groups may be perpetrators as well as targets of online crime. It provided an up-to-date analysis of the various online platforms used by cybercriminals as well as examined how these malevolent groups form, how their members develop trust in each other, and the motives that drive a group's success and actions. In addition to elucidating these often-undefined aspects in research, it also presented a characterization of the group element of cybercrime and its main types, including newly emerging group types. The current research forms the basis for a more thorough understanding of online criminal groups, and thereby encourages further discussions on how they might be unraveled and potentially even thwarted.

## References

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen da*ta. Hackers'* bazaar. Santa Monica, CA: RAND Corporation.

Aiken, M. P., & McMahon, C. (2014). The cyberpsychology of internet facilitated organised crime. In The Internet organised crime threat assessment report (iOCTA). The Hague: EUROPOL.

Bright, P. (2012, 7 March). Doxed: how Sabu was outed by former Anons long before his arrest. Ars Technica. Retrieved from https://arstechnica.com/tech-policy/2012/03/doxed-how-sabu-was-outed-by-former-anons-long-before-his-arrest/

Atkinson, S. (2015). Psychology and the hacker—Psychological Incident Handling. London: SANS Institute.

Awan, I. (2014). Islamophobia and Twitter: A typology of online hate against Muslims on social media. Policy & Internet 6(2), 133–150. doi: 10.1002/1944-2866.POI364

BBC. (2015). Ghost Security Group: Spying on Islamic State instead of hacking them. Retrieved February 6, 2018, from http://www.bbc.co.uk/news/blogs-trending-34879990

Bradbury, D. (2014). Unveiling the dark web. Network Security 2014(4), 14–17. doi: 10.1016/S1353-4858(14)70042-X

Best, J. & Luckenbill, D. F. (1994). Organizing Deviance (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cybercrime: An analysis of the nature of groups engaged in cybercrime. International Journal of Cyber Criminology 8(1), 1–20.

Bossler, A., & Burruss, G. (2010). The general theory of crime and computer hacking: Low self control hackers? In T. J. Holt & B. H. Schell (Eds.), Corporate hacking and technology-driven crime: Social dynamics and implications (pp. 38–67). Hershey, PA: IGI Global.

Engle, P. (2015, 21 November). *Inside the app that's become ISIS' biggest propaganda* machine. Business Insider. Retrieved from http://uk.businessinsider.com/telegram-isis-app-encrypted-propagandar-2015-11

Catakoglu, O., Balduzzi, M., & Balzarotti, B. (2017). Attacks landscape in the dark side of the web. In Proceedings of the Symposium on Applied Computing (pp. 1739–1746). 3–7 April, Marrakech, Morocco. New York: ACM. doi: 10.1145/3019612.3019796

CBS News. (2017). Behind the online community organizing protests against Trump. Retrieved from https://www.cbsnews.com/video/behind-the-online-community-organizing-protests-against-trump/

Chahal, K. (2016). Supporting victims of hate crime: A practitioner guide. Policy Press.

Chau, M., & Xu, J. (2007). Mining communities and their relationships in blogs: A study of online hate groups. International Journal of Human-Computer Studies 65(1), 57–70. doi: 10.1016/j.ijhcs.2006.08.009

Chiles, T. H., & McMackin, J. F., (1996). Integrating variable risk preferences, trust, and transaction cost economics. The Academy of Management Review 21(1), 73–99.

Choo, K. K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. Asian Journal of Criminology 3(1), 37–59. doi: 10.1007/s11417-007-9035-y

Cleland, J., Anderson, C., & Aldridge-Deacon, J. (2017). Islamophobia, war and non-Muslims as victims: An analysis of online discourse on an English Defence League message board. Ethnic and Racial Studies 41(9), 1–17. doi: 10.1080/01419870.2017.1287927

Cole, J., Watkins, C., & Kleine, D. (2016). Health advice from Internet discussion forums: How bad is dangerous? Journal of Medical Internet Research 18(1). doi: 10.2196/jmir.5051

Corritore, C., Kracher, B., & Wiedenbeck, S. (2003). Online trust: concepts, evolving themes, a model. International Journal of Human Computer Studies 58, 737–758. doi: 10.1016/S1071-5819(03)00041-7

Lenhart, A., Ybarra, M., Zickuhr K., & Price-Feeney, M. (2016). Online Harassment, Digital Abuse, and Cyberstalking in America. New York: Data & Society Research Institute. Retrieved from https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf

European Union Agency for Law Enforcement Co-operation. (2014). Internet Organised Crime Threat Assessment (iOCTA).

Falcone, R., Singh, M. P., & Tan, Y. H. (2001). Trust in cyber-societies: Integrating the human and artificial perspectives. New York: Springer.

FBI. (2016). Transnational organized crime. Retrieved from https://www.fbi.gov/investigate/organized-crime

FBI. (2015, 15 July). Cybercriminal forum taken down, members arrested in 20 countries. Retrieved from https://www.fbi.gov/news/stories/cyber-criminal-forum-taken-down

Finckenauer, J. O., and Voronin, Y. A. (2001). The threat of Russian organized crime (Vol. 2). Washington, DC: US Department of Justice, Office of Justice Programs, National Institute of Justice.

Frier, S. (2017, 27 January). Facebook groups, with 1 billion users, charts path to add more. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2016-01-27/facebook-groups-with-1-billion-users-charts-path-to-add-more

Fuchs, C. (2012). Social media, riots, and revolutions. Capital & Class 36(3), 383–391. doi: 10.1177/0309816812453613

Gambetta, D. (2009). Signalling. In: P. Hedstrom & P. Bearman (Eds.), The Oxford Handbook of Analytical Sociology (pp. 168–94). New York: OUP. doi: 10.1093/oxfordhb/9780199215362.013.8

Gerbaudo, P. (2012). Tweets and the streets: Social media and contemporary activism. London: Pluto Press.

Glaser, J., Dixit, J., & Green, D. P. (2002). Studying hate crime with the Internet: What makes racists advocate racial violence? Journal of Social Issues 58(1), 177–193. doi: 10.1111/1540-4560.00255

Godson, R. (2003). Transnational crime, corruption, and security. In: M. E. Brown (Ed.), Grave new world: Security challenges in the 21st century (pp. 259–278). Washington DC: Georgetown University Press.

Green, D. P., McFalls, L. H., & Smith, J. K. (2001). Hate crime: An emergent agenda. Annual Review of Sociology 27, 479–504. doi: 10.1146/annurev.soc.27.1.479

HM Treasury and Home Office. (2015). UK national risk assessment of money laundering and terrorist financing. Retrieved from https://www.gov.uk/government/publications/uk-national-risk-assessment-of-money-laundering-and-terrorist-financing

Hogg, M. A., & Williams, K. D. (2000). From I to we: Social identity and the collective self. Group Dynamics: Theory, Research, and Practice 4, 81. doi: 10.1037/1089-2699.4.1.81

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. Criminal Justice Studies 23(1), 33–50. doi: 10.1080/14786011003634415

Holt, T. J., & Smirnova, O. (2014). Examining the structure, organization, and processes of the international market for stolen data. Washington, DC: US Department of Justice.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. Global Crime 16, 81–103. doi: 10.1080/17440572.2015.1013211

Holtz, P., Kronberger, N., & Wagner, W. (2012). Analyzing internet forums: A practical guide. Journal of Media Psychology: Theories, Methods, and Applications 24(2), 55–66. doi: 10.1027/1864-1105/a000062

Hunt, J. G., & Hill, J. W. (1969). The new look in motivation theory for organizational research. Human Organization 28(2), 100–109. doi: 10.17730/humo.28.2.98302j32233wptg7

Schwartz, M. J. (2016). Anonymous threatens bank DDoS disruptions. [blog post]. Bankinfosecurity.com. Retrieved from http://www.bankinfosecurity.com/anonymous-threatens-bank-ddos-disruptions-a-9085

Billington, J. (2015, 17 December). Paris terrorists used WhatsApp and Telegram to plot attacks according to investigators. International Business Times. Retrieved from http://www.ibtimes.co.uk/paris-terrorists-used-whatsapp-telegram-plot-attacks-according-investigators-1533880

Klausen, J. (2015). Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq. Studies in Conflict & Terrorism 38(1), 1–22. doi: 10.1080/1057610X.2014.974948

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin 140(4), 1073–1137. doi: 10.1037/a0035618

Lacey, D., Salmon, P.M. (2015). It's dark in there: Using systems analysis to investigate trust and engagement in dark web forums. In: D. Harris (Ed.), Engineering Psychology and Cognitive Ergonomics. Cham: Springer. doi: 10.1007/978-3-319-20373-7_12

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016). A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. Crime, Law and Social Change 67(1), 21–37. doi: 10.1007/s10611-016-9662-2

Leukfeldt, E. R., Kleemans, E. R., & Stol, W.P. (2017). Origin, growth, and criminal capabilities of cybercriminal networks. An international empirical analysis. Crime, Law and Social Change 67(1), 39–53. doi: 10.1007/s10611-016-9663-1

Leukfeldt, E. R., de Poot, C., Verhoeven, M., & Lavorgna, A. (2017). Cybercriminal networks. In: R. Leukfeldt (Ed.), Research Agenda: The Human Factor in Cybercrime and Cybersecurity (pp. 33–42). The Hague: Eleven International.

Lu, Y., Luo, X., Polgar, M. & Cao, Y. (2010). Social Network Analysis of a Criminal Hacker Community. Journal of Computer Information Systems 51(2), 31–41.

Lusthaus, J. (2012). Trust in the World of Cybercrime. Global Crime 13(2), 71–94. doi: 10.1080/17440572.2012.674183

McCarthy, B., & Hagan, J., (2001). When crime pays: Capital, competence, and criminal success. Social Forces 79(3), 1035–1060.

Magdy, S. (2016). A safe space for terrorists. British Journalism Review 27(4), 23–28. doi: 10.1177/0956474816681736

Malenkovich, S. (2012, 7 December). What Motivates Cybercriminals? Money, Of Course. [blog post]. Kaspersky Lab. Retrieved from https://blog.kaspersky.com/what-motivates-cybercriminals-money-of-course/717/

Maslow, A. H. (1954). Motivation and Personality. New York: Harper and Row.

Mayer, R.C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review 20, 709–734. doi: 10.2307/258792

McGuire, M. (2012). Organized Crime in the Digital Age. London: John Grieve Centre for Policing and Security.

McDevitt, J., Levin, J., & Bennett, S. (2002). Hate crime offenders: an expanded typology. Journal of Social Issues 58(2), 303–17. doi: 10.1111/1540-4560.00262

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2008). Are blogs putting youth at risk for online sexual solicitation or harassment? Child Abuse & Neglect 32(2), 277–294. doi: 10.1016/j.chiabu.2007.04.015

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G.M. (2013). An analysis of underground forums. In Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement (pp. 71–79). 2–4 November, Berlin, Germany. New York: ACM. doi: 10.1145/2068816.2068824

Zorabedian, J. (2014, 26 August). "Lizard Squad" hackers force PSN offline and Sony exec from the sky. NakedSecurity. Retrieved from https://nakedsecurity.sophos.com/2014/08/26/lizard-squad-hackers-force-psn-offline-and-sony-exec-from-the-sky/

National Cyber Security Centre. (2017). Cyber crime: understanding the online business model. Retrieved from https://www.ncsc.gov.uk/news/ncsc-publishes-new-report-criminal-online-activity

Kushner, D. (2014). The Masked Avengers: How Anonymous incited online vigilantism from Tunisia to Ferguson. The New Yorker. Retrieved from http://www.newyorker.com/magazine/2014/09/08/masked-avengers

Hamill, J. (2017, 28 March). How terrorists use encrypted messaging apps to plot, recruit and attack. New York Post. Retrieved from http://nypost.com/2017/03/28/how-terrorists-use-encrypted-messaging-apps-to-plot-recruit-and-attack/

Norton, Q. (2012, 3 July). How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down. Wired. Retrieved from https://www.wired.com/2012/07/ff_anonymous/

Nouh, M., & Nurse, J. R. C. (2015). Identifying key-players in online activist groups on the Facebook Social Network. In Proceedings of the International Conference on Data Mining Workshop (ICDMW) (pp. 969–978). 14–17 November, Atlantic City, New Jersey. Sandy Hook, NY: Curran Associates. doi: 10.1109/ICDMW.2015.88

Nouh, M., Nurse, J. R. C., & Goldsmith, M. (2016). Towards designing a multipurpose cybercrime intelligence framework. In Proceedings of the European Intelligence and Security Informatics Conference (EISIC) (pp. 60–67). 17–19 August, Uppsala, Sweden. Sandy Hook, NY: Curran Associates. doi: 10.1109/EISIC.2016.018

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. & Whitty, M., (2014). Understanding insider threat: A framework for characterising attacks. In Proceedings of the IEEE Security and Privacy Workshops (SPW) (pp. 214–228). 17–18 May, San Jose, California. doi: 10.1109/SPW.2014.38

Nurse, J. R. C., Rahman, S. S., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Information quality and trustworthiness: a topical state-of-the-art review. In Proceedings of the International Conference on Computer Applications and Network Security (ICCANS) (pp. 492–500). 27-29 May, Maldives. Sandy Hook, NY: Curran Associates.

Odinot, G., Verhoeven, M.A., Pool, R.L.D. & De Poot, C.J. (2016). Cybercrime, organised crime and organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement. The Hague: WODC.

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. Vulnerable Children and Youth Studies 8(4), 298–309. doi: 10.1080/17450128.2012.752119

Olson, P. (2013). We are Anonymous. New York: Random House.

Perry, B., & Olsson, P. (2009). Cyberhate: The globalisation of hate. Information & Communications Technology Law 18(2), 185–199. doi: 10.1080/13600830902814984

Reicher, Stephen. (2001). The Psychology of Crowd Dynamics. In M. A. Hogg & S. Tindale (Eds.), Blackwell Handbook of Social Psychology: Group Processes (pp. 182–208). Malden, MA: Blackwell Publishers.

Richardson, R., (2007). CSI Survey 2007: The 12th Annual Computer Crime and Security Survey. San Francisco, CA: Computer Security Institute.

Rieker, P. (1997). Ethnozentrismus bei jungen Mannern. Weinheim: Juventa.

Rodgers, L. (2007, 20 December). Smashing the criminal's e-bazaar. BBC News Online. Retrieved from http://news.bbc.co.uk/1/hi/uk/7084592.stm

Rogers, M.K. (2006). A Two-dimensional circumplex approach to the development of a hacker taxonomy. Digital Investigations 3(2), 97–102. doi: 10.1016/j.diin.2006.03.001

Metzger, M. (2017, 18 January). Update: Old fashioned DDoS attack planned to protest Trump's inauguration. SC Media UK. Retrieved from https://www.scmagazineuk.com/update-old-fashioned-ddos-attack-planned-to-protest-trumps-inauguration/article/632195/

Shinder, D. (2010, 19 July). Profiling and categorizing cybercriminals. TechRepublic. [blog post]. Retrieved from http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069

Longbottom, W. (2017, 21 January). Protests in Washington after Trump inauguration: Tear gas and stun grenades. SkyNews. Retrieved from http://news.sky.com/story/anti-trump-protesters-smash-windows-in-tense-scenes-before-inauguration-10735956

Stott, C., Drury, J., & Reicher, S. (2016). On the role of a social identity analysis in articulating structure and collective action: The 2011 riots in Tottenham and Hackney. The British Journal of Criminology 57(4), 964–981. doi: 10.1093/bjc/azw036

Arthur, C. (2013, 16 May). LulzSec: what they did, who they were and how they were caught. The Guardian. Retrieved from https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail

Woolf, N. (2016, 24 March). Anti-Trump campaign sparks civil war among Anonymous hackers. The Guardian. Retrieved from

https://www.theguardian.com/technology/2016/mar/24/anti-donald-trump-campaign-anonymous-hackers-debate-election-2016

Robins-Early, N. (2017, 24 May). How Telegram became the app of choice for ISIS. The Huffington Post. Retrieved from http://www.huffingtonpost.co.uk/entry/isis-telegram-app_us_59259254e4b0ec129d3136d5

Griffin, A. (2015). Paris attack: Anonymous launches biggest operations ever against ISIS. The Independent. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/paris-attacks-anonymous-launches-its-biggest-operation-ever-against-isis-promises-to-hunt-down-a6735811.html

Griffin, A. (2017). Anonymous tells supporters use tools given by them to attack Donald Trump. The Independent. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-donald-trump-twitter-optrump-opdeatheaters-russia-dossier-information-a7530966.html

Rayner, G. (2017). WhatsApp accused of giving terrorists “a secret place to hide” as it refuses to hand over London attacker’s messages. The Telegraph. Retrieved from http://www.telegraph.co.uk/news/2017/03/26/home-secretary-amber-rudd-whatsapp-gives-terrorists-place-hide/

Thibaut, J., & Kelley, H. H. (1959). The Social Psychology of Groups. New York: Wiley.

Peckham, M. (2012, 20 January). 10 Sites Skewered by Anonymous, Including FBI, DOJ, U.S. Copyright Office. Time. Retrieved from http://techland.time.com/2012/01/20/10-sites-skewered-by-anonymous-including-fbi-doj-u-s-copyright-office/

TrendMicro Inc. (2016, 3 May). Dark Motives Online: An Analysis of Overlapping Technologies Used by Cybercriminals and Terrorist Organizations. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/overlapping-technologies-cybercriminals-and-terrorist-organizations

United Nations Office on Drugs and Crime. (2002). Global Programme Against Transnational Organized Crime. Vienna, Austria. Retrieved from http://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf

Van Der Broek, T. C., Van der Laan, A. M. & Weijters, G. (2016). Bedreiging via internet: Verschillen in risicofactoren tussen jongeren die online en offline bedreigen. Panopticon, tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk 37(2), 90–105.

Vromen, A., Xenos, M. A., & Loader, B. (2015). Young people, social media, and connective action: From organisational maintenance to everyday political talk. Journal of Youth Studies 18(1), 80–100. doi: 10.1080/13676261.2014.933198

Wall, D. (2007). Cybercrime: The transformation of crime in the information age. Cambridge: Polity.

Wall, D. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. The European Review of Organised Crime 2(2), 71–90.

Wasserman, S., & Faust, K. (1994). Social network analysis: Methods and applications. Cambridge: CUP.

Williams, M., Axon, L., Nurse, J. R. C., & Creese, S. (2016). Future scenarios and challenges for security and privacy. In Proceedings of the IEEE 2nd International Forum on Research and Technologies for Society and Industry: Leveraging a better tomorrow (RTSI) (pp. 1–6). 7–9 September, Bologna, Italy. Red Hook, NY: Curran Associates. doi: 10.1109/RTSI.2016.7740625

Yip. M., Shadbolt, N., & Webber, C. (2013). Why forums? An empirical analysis into the facilitating factors of carding forums. In Proceedings of the 5th Annual ACM Web Science Conference (pp. 453–462). 2–4 May, Paris, France. New York: ACM. doi: 10.1145/2464464.2464524

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. Policing & Society 23(4), 516–539. doi: 10.1080/10439463.2013.780227

Yunus, M. M., & Salehi, H. (2012). The effectiveness of Facebook groups on teaching and improving writing: Students' perceptions. Journal of Education and Information Technologies 1(6), 87–96.

**Table 1**

**The group element of cybercrime and its main types.**

| **Main group types** | **Group subtypes** |
|---|---|
| Groups as perpetrators | • Traditional organized crime groups that use technology to enable crime.<br>• Organized cybercriminal groups.<br>• Organized ideologically and politically motivated cyber groups.<br>• Citizen groups that use technology to mobilize and act. |
| Groups as victims | • Race<br>• Age<br>• Disability<br>• Religion/belief<br>• Sex<br>• Sexual orientation |