



Rivista di Criminologia, Vittimologia e Sicurezza

*Organo ufficiale della
Società Italiana di Vittimologia (S.I.V.)*

*World Society of Victimology (WSV)
Affiliated Journal*

Anno XVI

Gennaio-Dicembre 2022

Numero Unico

Numero curato da Giorgia Macilotti e Sandra Sicurella

Rivista di Criminologia, Vittimologia e Sicurezza

Rivista quadrimestrale fondata a Bologna nel 2007

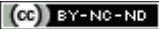
ISSN: 1971-033X

Registrazione n. 7728 del 14/2/2007 presso il Tribunale di Bologna

Redazione e amministrazione: Società Italiana di Vittimologia (S.I.V.) - Via Sant'Isaia 8 - 40123 Bologna - Italia; Tel. e Fax. +39-051-585709; e-mail: augustoballoni@virgilio.it

Rivista peer reviewed (procedura double-blind) e indicizzata su:

Catalogo italiano dei periodici/ACNP, Progetto CNR SOLAR (Scientific Open-access Literature Archive and Repository), directory internazionale delle riviste open access DOAJ (Directory of Open Access Journals), CrossRef, ScienceOpen, Google Scholar, EBSCO Discovery Service, Academic Journal Database, InfoBase Index

Tutti gli articoli pubblicati su questa Rivista sono distribuiti con licenza Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License 

Editore e Direttore: **Augusto BALLONI**, presidente S.I.V., già professore ordinario di criminologia, Università di Bologna, Italia (direzione@vittimologia.it)

COMITATO EDITORIALE

Coordinatore: **Raffaella SETTE**, dottore di ricerca in criminologia, professore associato, Università di Bologna, Italia (redazione@vittimologia.it)

Francesco AMICI (Università di Parma), Elena BIANCHINI (Università di Bologna), Roberta BIOLCATTI (Università di Bologna), Luca CIMINO (Università di Bologna), Lorenzo Maria CORVUCCI (Foro di Bologna), Emilia FERONE (Università "G. D'Annunzio", Chieti-Pescara), Francesco FERZETTI (Università "G. D'Annunzio", Chieti-Pescara), Maria Pia GIUFFRIDA (Associazione Spondé), Giorgia MACILOTTI (Università Tolosa 1 Capitole, Francia), Andrea PITASI (Università "G. D'Annunzio, Chieti-Pescara), Anna ROVESTI (Studio Consulenza Lavoro dal Bon, Modena), Sandra SICURELLA (Università di Bologna)

COMITATO SCIENTIFICO

Coordinatore: **Roberta BISI**, vice Presidente S.I.V., professore ordinario di sociologia della devianza, Università di Bologna, Italia (comitatoscientifico@vittimologia.it)

Andrea BIXIO (Università Roma "La Sapienza"), Encarna BODELON (Università Autonoma di Barcellona, Spagna), Stefano CANESTRARI (Università di Bologna), Laura CAVANA (Università di Bologna), Gyorgy CSEPELI (Institute of Advanced Studies Koszeg, Ungheria), Janina CZAPSKA (Università Jagiellonian, Cracovia, Polonia), Lucio D'ALESSANDRO (Università degli Studi Suor Orsola Benincasa, Napoli), François DIEU (Università Tolosa 1 Capitole, Francia), Maria Rosa DOMINICI (S.I.V.), John DUSSICH (California State University, Fresno), Jacques FARSEDAKIS (Università Europea, Cipro), André FOLLONI (Pontifical Catholic University of Paraná, Brasile), Ruth FREEMAN (University of Dundee, UK), Paul FRIDAY (University of North Carolina, Charlotte), Shubha GHOSH (Syracuse University College of Law, USA), Xavier LATOUR (Université Côte d'Azur), Jean-Marie LEMAIRE (Institut Liégeois de Thérapie Familiale, Belgio), André LEMAÏTRE (Università di Liegi, Belgio), Silvio LUGNANO (Università degli Studi Suor Orsola Benincasa, Napoli), Mario MAESTRI (Società Psicoanalitica Italiana, Bologna), Luis Rodriguez MANZANERA (Università Nazionale Autonoma del Messico), Gemma MAROTTA (Sapienza Università di Roma), Vincenzo MASTRONARDI (Unitelma-Sapienza, Roma), Maria Rosa MONDINI (Centro Italiano di Mediazione e Formazione alla Mediazione, Bologna), Stephan PARMENTIER (Università Cattolica, Lovanio, Belgio), Tony PETERS† (Università Cattolica, Lovanio, Belgio), Monica RAITERI (Università di Macerata), Francesco SIDOTI (Università de l'Aquila), Philip STENNING (Università di Griffith, Australia), Liborio STUPPIA (Università "G. D'Annunzio, Chieti-Pescara), Emilio VIANO (American University, Washington, D.C.), Sachio YAMAGUCHI (Università Nihon Fukushi, Giappone), Simona ZAAMI (Università Roma "La Sapienza"), Christina ZARAFONITOU (Università Panteion, Atene), Vito ZINCANI (Procura della Repubblica, Modena), Vladimir ZOLOTYKH (Udmurt State University, Russia)

Editoriale. Il sapere criminologico tra rischi e opportunità
di *Augusto Balloni*

pag. 4

Le nuove sfide delle cybercriminalità e delle forme di controllo sociale

Criminalità e cyberspazio, alcune riflessioni in materia di cybercriminalità

di *Maurizio Tonello*

pag. 6

doi: 10.14664/rcvs/240

Le mafie italiane nel cyberspazio: nuova frontiera o terreno di sperimentazione?

di *Sandra Sicurella*

pag. 22

doi: 10.14664/rcvs/241

Hactivists from the Inside: Collective Identity, Target Selection and Tactical Use of Media during the Quebec Maple Spring Protests

di *Francis Fortin, Francesco C. Campisi, Marie-Ève Néron*

pag. 35

doi: 10.14664/rcvs/242

Les atteintes à l'image en Turquie : étude de cas d'un fléau numérique ravageur

di *Julie Alev Dilmaç, Verda Irtiş*

pag. 57

doi: 10.14664/rcvs/243

Le renseignement criminel au service de la lutte contre la cybercriminalité : l'exemple français de la gendarmerie nationale

di *Jérôme Barlatier*

pag. 91

doi: 10.14664/rcvs/244

Cybercriminalité et pluralisation du *policing* : la *cyber threat intelligence* en question

di *Camille Guisset, Giorgia Macilotti*

pag. 116

doi: 10.14664/rcvs/245

Varia

Age and crime: Empirical and theoretical approaches of criminal adult onset

di *Eleni Kontopoulou*

pag. 136

doi: 10.14664/rcvs/246

Children of imprisoned parents. An Italian and European analysis

di *Sara Fontanot*

pag. 148

doi: 10.14664/rcvs/247

Crimini ambientali ed ecomafie: un argomento criminologico tuttora complesso

di *Eleonora Medina*

pag. 167

doi: 10.14664/rcvs/248

Agli albori della prevenzione situazionale: l'attualità dei sostitutivi penali di Enrico Ferri

di *Natalia Coppolino*

pag. 196

doi: 10.14664/rcvs/249

Gli hacktivististi dall'interno: identità collettiva, selezione degli obiettivi e uso tattico dei media durante le proteste della Primavera dell'Acero in Québec

Les hacktivistes de l'intérieur : identité collective, sélection des cibles et utilisation tactique des médias pendant les manifestations du Printemps Érable au Québec

Hactivists from the Inside: Collective Identity, Target Selection and Tactical Use of Media during the Quebec Maple Spring Protests

*Francis Fortin**, *Francesco C. Campisi***, and *Marie-Ève Néron****

Riassunto

La maggior parte delle ricerche su Anonymous ha studiato il gruppo da un punto di vista etnografico o si è concentrata sull'analisi dei messaggi diffusi sui social media per comprendere gli interessi del movimento. Ci sono stati pochi tentativi di analizzare il modo in cui gli hacktivististi scelgono gli obiettivi appropriati per gli attacchi informatici a fini di protesta. Il presente studio cerca di fornire una panoramica dei valori condivisi da Anonymous esaminando le interazioni tra i membri del gruppo nelle chat room pubbliche durante i quattro mesi delle manifestazioni studentesche in Québec conosciute come *Primavera dell'Acero 2012*. In tal senso, è stata effettuata un'analisi tematica al fine di identificare i temi importanti. I risultati mostrano che i valori fondamentali di Anonymous sono coerenti con quelli diffusi attraverso gli account social media del gruppo, focalizzandosi in particolare sulla libertà di espressione spesso legata alla libertà di parola e di informazione come parte integrante del processo di selezione degli obiettivi. L'analisi mostra inoltre come i partecipanti alle chat abbiano proposto dei bersagli tipici dell'attivismo politico (ad esempio, il governo, la polizia, i partiti politici) e siano concordi sugli obiettivi da rifiutare, come i mezzi d'informazione tradizionali, in quanto considerati importanti per la diffusione dei messaggi del gruppo e delle informazioni relative alle operazioni svolte.

Résumé

Une grande partie de la recherche sur Anonymous a étudié le groupe d'un point de vue ethnographique ou s'est concentrée sur les messages des médias sociaux pour apprendre ce qui est le plus important pour le mouvement. Il n'y a eu que peu de tentatives d'analyse de la manière dont les hacktivistes choisissent les cibles appropriées pour les cyberattaques ayant des objectifs de protestation. La présente étude tente de donner un aperçu des valeurs partagées en examinant les interactions entre les membres d'Anonymous sur les salons de discussion publics pendant les quatre mois des manifestations étudiantes québécoises connues sous le nom de Printemps Érable 2012. Une analyse thématique a été réalisée pour catégoriser les thèmes importants. Les résultats montrent que les valeurs fondamentales du groupe Anonymous sont congruentes à celles des comptes de médias sociaux d'Anonymous, mettant l'accent sur la liberté d'expression, souvent liée à la liberté de parole et à la liberté d'information comme partie intégrante du processus de sélection des cibles. En outre, les participants au salon de discussion ont proposé des cibles traditionnellement appropriées (c'est-à-dire le gouvernement, la police, les partis politiques) et semblent s'accorder sur les cibles à rejeter, comme les médias d'information traditionnels, jugés importants pour diffuser son message et fournir des informations sur ses opérations.

Abstract

Much of the research on Anonymous has studied the group from an ethnographic perspective or focused on social media posts to learn what is most important for the movement. There have been only few attempts to analyze how hacktivists are choosing suitable targets for cyberattacks with protest objectives. The present study attempts to provide insight into their shared values by looking at interactions among Anonymous members on public chatrooms during the four months of the

* Ph.D., School of criminology, University of Montreal.

** M.A., Ph.D. candidate, School of criminology, University of Montreal.

*** M.Sc., School of criminology, University of Montreal.

Quebec student demonstrations known as the 2012 *Printemps Érablé* protests. A thematic analysis was performed to categorize the important themes. The results show that the core values of Anonymous's group is congruent to that of Anonymous's social media accounts, emphasizing freedom of expression, often linked to freedom of speech and freedom of information as integral to the target selection process. Also, participants in the chatroom proposed traditionally suitable targets (i.e., the government, the police, political parties) and seems to agree upon which targets should be rejected such as traditional news media, deemed important to diffuse its message and provide information about its operations.

Key words: hacktivism, Anonymous, online disobedience, values, cybercrime

1. Introduction¹

In April 2012, an ominous video was published on YouTube. The video, projecting a man in a suit donning a Guy Fawkes mask spoke to the camera and stated the government of Québec's emergency law will "assassinate the right to protest" (Levesque, 2012, p. 1). The law in question, Bill-78, was, at that time, being discussed on the floor of the Quebec National Assembly as a response to the ongoing student protests. A month prior, the Liberal Party of Quebec announced a 75% tuition increase for CEGEP (Quebec publicly funded colleges) and university students across the province (Raynauld *et al.*, 2016). This caused students to protest on the streets, blocking entrances to university buildings, and clash with police over the course of several months. These protests, known as the Maple Spring or *le Printemps Érablé* (in French), received national attention, attracting several thousand students to take part in voicing their concerns and outright opposition towards the tuition increase (Raynauld *et al.*, 2016). In response, Bill-78 proposed limitations on student protests by outlawing all rallies containing 50 people or more, unless the rallies were approved by police, as well as granting greater discretionary powers to police officers to control the crowds (Bégin-Caouette, Jones, 2014).

The Anonymous collective has been a trailblazer in the hacktivist movement, since its first involvement

with social and political causes in 2008. For the purposes of this study, the term hacktivism is defined as the hybridization of computer technology and social activism (Gunkel, 2005). Hacktivists like Anonymous use a wide variety of hacker-typed techniques (website defacement, distributed denial of service attacks, virtual sit-ins and leaking classified documents, to name a few) for the purposes of disrupting, creating harm, bringing attention to a social movement or cause, and putting pressures on traditional institutions of power (Caldwell, 2015; Gunkel, 2005; Kelly, 2012; Renzi, 2015). Over the years, Anonymous has utilised these techniques (most notably DDoS attacks and website defacement) against institutions they deemed to have infringed on both individual and collective freedoms (Bardeau, Danet, 2011; Beyer, 2014; Coleman, 2014). Bill-78 and the Québec government were no exception. While the Anonymous cell in the province of Québec initially refrained from their involvement, it was the introduction of Bill-78 that sparked #OperationQuébec, where Anonymous members hacked several government and police websites between the months of April and May 2012.

The cyberattacks on the Québec government are representative of similar Anonymous campaigns spanning over a decade. Anonymous has pursued governments, religious institutions, and other targets who they deem to infringe on freedoms such as the freedom of expression, freedom of information, and individuals' ability to protest (Jones *et al.*, 2020; Pendergrass, 2013). For example,

¹ This study was funded through a Social Sciences and Humanities Research Council of Canada (SSHRC) grant (SSHRC/CRSH #430-2016-01048).

Operation Paris was an Anonymous campaign against ISIS, after a series of Islamist terrorist attacks that took place in a suburb of Paris and at soccer stadium in St-Denis on November 13, 2015 (de la Hamaide, 2015). This trend has remained stable over time, as Anonymous has more recently targeted American police forces and the Russian government, who, according to Anonymous social media accounts, demonstrated abuses in powers (Franceschi-Bicchierai, 2020; Purtill, 2022). And thusly, the consistency of targets chosen for cyber attacks is reflected in a consistency of values and collective identity advocated on social media.

Yet little is known about the values of those Anonymous members engaging in both the target selection process and the hacking operations themselves. This is due to both the secretive nature of the target selection process and the plethora of information Anonymous divulges on social media. Research has primarily analysed Anonymous' social media accounts as they provide information on different campaigns, successful hacking operations and social causes (Bergeron *et al.*, 2019; McGovern, Fortin, 2019). As such, values attributed to Anonymous stem from an interpretation of these sources, suggesting a cohesion of collective identity and values among the two strata of members: the hackers and the social media users. However, due to Anonymous' nebulous and informal structure, there is little evidence to suggest that the members hacking government websites and those operating social media are one and the same. For example, Anonymous's 'accept-all' strategy for membership allows for individuals with different goals and technical skills to participate (Kelly, 2012). Based on these characteristics, members can participate uniquely through social media if they so choose,

raising questions as to the possible disconnect in values between hackers and other members.

The present study analyses the activities of Anonymous' Québec cell participants on two public chatrooms during the Maple Spring to determine which values were most important to Anonymous' hackers during their target selection process. This objective is significant due to Anonymous's loosely defined structure and addresses questions regarding their ability to organise post 2011. At the end of 2011, one of Anonymous's leader, known online as Sabu, was arrested, which consequently resulted in the dissolution of the more militant arms of Anonymous: LulzSec and AntiSec (Anderson, 2012). This has had an undesirable effect, causing Anonymous to cluster, more so than they already loosely connected, informal structure for which they are known for. Anonymous post-Sabu has been characterised as much more ineffective at organising, with less clear motivations, often ending in dissent and confusion over messages, operations, and target selection (Kelly, 2012). It is therefore imperative to analyze Anonymous's communications during operations to ascertain Anonymous' values during the target selection process rather than through social media posts.

2. Literature Review

The first use of the term *hacktivism* originates in the late 1990s, by an American hacker under the pseudonym Omega; a member of the activist group called the Cult of the Dead Cow (CDC) (Guiton, 2013). The term itself is an amalgamation of the terms "hacking" and "activism", which refers to the use of computer technology as the predominant physical tool for advancing the political causes of a given movement (Conway, 2003; Denning, 2001; Gunkel, 2005; Ludlow, 2010; Manion, Goodrum,

2000). Contrary to traditional protest movements, hacktivism generally occurs when triggered by a social event/policy or when a social protest shows signs of repression from traditional institutions of power (George, Leidner, 2019; Kahn, Kellner, 2004). This denotes a symbiotic interplay between social movements and hacktivism; as hacktivism frequently work together with more traditional social movements, differing mainly on the techniques utilised.

With the aid of computer technologies, traditional social movements employ tactics defined as electronic civil disobedience, which are *generally* legal means of online protest and expressions [emphasis added] (Karatzogianni, 2013). According to George and Leidner (2019), electronic civil disobedience is considered part of digital transitional activities, in which offline forms of protests have transitioned into digital equivalencies (like virtual sit-ins, online petitions, etc.). Comparatively, hacktivism is categorized as digital gladiatorial activity, in which hacktivists perform more direct actions which may have more potential impacts on society, government and organisations (George, Leidner, 2019). A clearer taxonomy of hacktivism is presented by Samuel Houghton (see Romagna, 2020), who argues electronic civil disobedience is one small aspect of hacktivism, subcategorising hacktivism into three: political cracking, performative hacktivism and political coding. The first is the most aggressive form of hacktivism, such as website defacements, cyber trespassing, and DDoS attacks. The second, performative hacktivism, entails civil disobedience actions that are undertaken but not necessarily illegal, such as virtual sit-ins. The third, political coding is the development of software for political use, like the creation and modification of VPN and IRC forums. What englobes these categorisations is

the view of hacktivism as actionable, one where the type of actions requires computational technologies, and whose motivations stem from political or social tensions and events.

In general, due to the flexible definition of hacktivism, research has compiled hacktivist activities to include virtual sit-ins, website disfiguration, email bombing, site parodies, distributed denial of service attacks (DDoS attacks), disclosure of hacked confidential information, site parodies and assertions on social media (Auty, 2004; Caldwell, 2015; George, Leidner, 2019; Hampson, 2012; Karatzogianni, 2013; Li, 2013; West, 2017). Despite the multitude of techniques presented, an important technique in hacktivists' repertoire is that of assertion. Assertion is frequently used as a tool for dissemination of information, which range from posting content regarding certain hacktivist operations taking place on other platforms, interacting with citizens, other activists, and commentating on government activities (George, Leidner, 2019). This tactical form of media usage allows for hacktivists to critique powerful regimes by exposing temporary fissures of power and disrupt the incumbent power through online exposure (McKelvey, 2010).

The ability to demystify Anonymous' values is a direct result of assertion, as Anonymous is highly active on social media. Anonymous members write press communiqués, media interviews, and publish content that makes propaganda, videos, and information on social causes publicly accessible (Coleman, 2020). Individual members are running hundreds of Anonymous Twitter accounts, using social media to broker and connect individuals and social movements, using bots to boost visibility, and influence greater support for a cause (Beraldo, 2022; Jones *et al.*, 2022). Anonymous values are also

extracted through an analysis of the content produced on social media. For example, an analysis of hashtag usage found that male and female members focused on animal rights, conspiracy theories, and ISIS (McGovern, Fortin, 2019). The hacks themselves are often evaluated by the media, citing the Anonymous-affiliated tweets to best understand their motivations and goals (Bonifacic, 2022; Kika, 2022; Papadopoulos, 2022). The tactical use of both social and mass media forces discourse by presenting a contrasting vision of justice and freedom, challenging these notions for the purposes of changing longstanding control by governments and other institutions of power. As such, their use of assertion both implicitly and explicitly reveals the values that motivate their target selection.

2.1 Collective Identity

What makes Anonymous enigmatic is its unparalleled ability to launch hundreds of online campaigns, despite its lack of defined shape and its imprecise, nebulous structure. This makes it hard to identify how it shapes the collective identity of its members (Machado, 2015; Mansfield-Devine, 2011). As one author notes, “Even under the discrete umbrella of hacktivism, [...] Anonymous has a distinct makeup: a decentralised (almost nonexistent) structure, unabashed moralistic/political motivations, and a proclivity to a couple online cyberattacks and offline protests” (Kelly, 2012, p. 1678). It is possible the fluid nature of the group’s structure contributes to the continued life of the movement, even after the arrests of its leaders (the infamous Hector “Sabu” Monsegur) and the subsequent dissolution of Anonymous’s affinity groups: LulzSec and AntiSec in 2011 (Anderson, 2012). Anonymous members (self-proclaimed “Anons”) do not operate within a

formal hierarchical power structure but instead create many small, horizontally structured groups, which allowed the movement to remain active even when faced with potential arrests and the loss of one or more of its more influential participants (Beran, 2020).

2.2 Freedom of Expression

Anonymous has a long history of targeting individuals and corporations who would place limitations on individual and collective freedoms. Initially, the members of Anonymous were seen as online pranksters (otherwise known as trolls) and their actions were viewed as disruptive by its victims and amusing by its members. For example, one of their first operations known as *Habbo Raid*, involved organising 4chan users to perform a virtual sit-in in the virtual world game Habbo Hotel (Bardeau, Danet, 2011). This operation was a performative prank aimed simply to block access to other users of the game — disruption for the sake of disruption. In 2008, in what came to be known as Project Chanology, attacks against the Church of Scientology increased the group’s visibility outside the message boards, and led to the evolution of the group as hacktivists, beginning to take on more social, political, economic and technological issues spanning several years (Caldwell, 2015; Coleman, 2011, 2014). Since that time, Anonymous members have used DDoS attacks and the leaking of confidential information against targets such as the America Israel Public Affairs Committee, the CIA, the FBI, the Vatican, the White House and the Westboro Baptist Church (Bodó, 2014; Kenney, 2015; Ludlow, 2010). Anonymous has been credited with publicly leading the hacktivist movement (*movement* being defined as the concept of hacktivism, not an organised social movement in

itself), utilising legal and illegal digital tools to pursue political actions and influence public opinion on a wide range of issues (Kelly, 2012; Pendergrass, 2013).

The quasi-homogenous group of targets chosen by Anonymous campaigns over the years are representative of their commitment to freedom of expression as a core value. Between 2008 to 2011, during the height of Anonymous's popularity, Anonymous's operations and members adhered to a specific philosophy, which englobed free access of information, ensuring that information remains both free and decentralised (Ludlow, 2010). Congruent with hacktivist goals as defined by Gunkel (2005) and Renzi (2015), the core values of Anons places them in opposition to those who try to curb freedom of expression and information sharing and defend the principles and values of anti-globalisation (Bardeau, Danet, 2011). Most recently, Anonymous pursued Russian governmental infrastructure, disfiguring websites affiliated to Russian State TV, Russia's space research institute, energy companies and the Center for the Protection of Monuments in response to perceived illegitimate invasion of the Ukraine by Russian forces (Everington, 2022; Faife, 2022). In each case, Anonymous targeted institutions and corporations who would place limitations on the individual and/or collective freedoms, particularly that of freedom of expression.

2.3 Immunity of the media

At its simplest, the tactical use of media and other hacking methods is crucial to the movement: hacktivism is a way of gaining visibility and causing harm (Caldwell, 2015; West, 2017). The use of these tactics suggests the willingness to garner attention to a social-political issue, raise awareness (due perhaps

to waning or neglecting attention), create public pressures, question established systems and, in a sense, resist the legitimisation of such institutions (Gunkel, 2005; Kelly, 2012; Renzi, 2015). As Renzi (2015) suggests, hacktivism creates a terrain for forced discourse by presenting a contrasting vision of justice and freedom, challenging these notions for the purpose of changing the longstanding, standardized control over those discourse by governments and other institutional forms of power. For example, Anonymous aided in publicizing rape cases in Ohio at an international level as well as aiding the Arab Spring protests when the government banned Twitter to its citizens (Coleman, 2020). As is the case with other social movements, hacktivism relies on mass media and social media to reach greater audiences and support, that overcome geographic limitations and suppressive means of the government. As such, the media, both traditional forms of media (e.g.: news sources) as well as social media, are imperative tools for hacktivist groups such as Anonymous, granting a certain immunity from hacktivist groups.

3. Aim of the study

There exist contradictions regarding Anonymous' organisational structure and its impact in the target selection process. Since the arrests of Anonymous leaders in late 2011 and early 2012, Anonymous has been deemed as weak and less effective than its past. Social movement researchers have noted campaigns rife with constant dissent over messages and operation targets, which is a direct consequence of its informal, decentralised structure (Caldwell, 2015; Kelly, 2012). Consequently, this has caused a blur in the target selection process, and the values which motivate certain operations such as minority-led projects and hacks, with no minimum approval,

and almost no justification between members (Kelly, 2012). For example, a lone anti-abortion hacker targeted Britain's largest abortion clinic under the banner of Anonymous (Coleman, 2020). While the campaign was disavowed by other Anonymous members and social media accounts, it is indicative of contradicting values motivating hackers during the target selection process due to the decentralised structure.

Yet the group has continued to mount kindred operations across the world, indicative of Anonymous' commitment to various freedoms and values, such as free access to information, freedom of expression and information sharing, and defending the principle and values of anti-globalisation against repressive regimes (Bardeau, Danet, 2011; Ludlow, 2010; Mansfield-Devine, 2011). For example, #OperationParis saw the hacking of hundreds of ISIS websites, shutting them down in an effort to quell the spread of false information and extremism online (McCrow-Young, Mortensen, 2021). During #OperationMinneapolis, Anons began hacking police services, publishing police officers' personal information on social media for harassment (known as *doxing*) and shutting down the Minneapolis Police Department websites after the death of George Floyd, a black Minneapolis man, at the hands of several police officers in 2020 (Castrodale, 2020; Franceschi-Bicchierai, 2020; Molloy, Tidy, 2020). Most recently, #OperationRussia included hacking several government websites as a response to the Russia- Ukraine war, to which Anonymous social media accounts deem as an illegal invasion (Everington, 2022; Faife, 2022).

The objectives of the present study are firstly, to assess mentions of a value system attributed to the hackers, and secondly to analyse communication

in Anon internet relay chatrooms (IRC) to determine the ways in which Anonymous hackers choose their targets. In doing so, this study is contextualising itself during the 2012 Québec Maple Spring, as the timeline places the events post-Sabu, when Anonymous was characterised as more disorganised, and rife with dissent and confusion over messages, values, operations and target selections (Caldwell, 2015; Kelly, 2012). This study therefore will present the communications amongst Anonymous Québec members to determine if a congruency between Anonymous social media promoted values and those discussed in the chatrooms. This qualitative analysis has been used in the past to evaluate message posted on social media, looking at their official communications (via social networking sites like Twitter) as a way to better understand what is important to the movement (McGovern, Fortin, 2019). However, those communications are generally among Anonymous social media administrators and their social media followers, not all of which are active participants in hacking or target selection process. A post-hoc interpretation of the targets attacked, as well as values promoted by individuals who may not have participated in target selection creates a disconnect in our understanding of Anonymous' values at both stages of hacktivism: the hack and assertion.

While the data of Anonymous IRC has to be nuanced within its temporal context, its impact regarding our fundamental understanding of Anonymous' values, and hacktivism is not to be underestimated. Firstly, this is due to the limited data regarding the target selection process prior to the cyberattacks. According to Coleman (2020), Anonymous operations are often reactive, making it difficult to obtain conversations in IRC, granting

greater significance to the limited data that is available for analysis. Secondly, the consistent targets chosen in Anonymous campaigns suggests the continued relevance of the data. Given this perennial stability in targets chosen, we remain confident that the results derived from the forums can be generalised to other campaigns even those that have recently taken place.

Analyzing the ways Anonymous' values function in operation and target selection is vitally important in understanding the continued relevance of hacktivism worldwide. Since 2012, cybersecurity experts have warned of the increase in hacktivist operations around the world (AFP, 2017; Caldwell, 2015; Canadian Centre for Cyber Security, 2018). While the Maple Spring was one of the first Anonymous operations on Canadian soil, it was not the last. During the 2015 federal elections, Anonymous was the subject of controversy as they were credited for a number of hacks, having leaked confidential government documents from the Canadian Treasury Board with several news outlets (MacLellan, 2018). The documents revealed information regarding foreign spy stations, and Canadian government secrets of varying levels of importance in order to disparage the Canadian Conservative government, under the leadership of Canadian Prime Minister Steven Harper (AFP, 2017; MacLellan, 2018). These examples, among others, demonstrates the importance of ongoing research on Anonymous operations, as both Anonymous and hacktivist operations are not a thing of the past.

4. Methodology

4.1 Data

The main source of data for the present research derives from the content of two public chatrooms

used by the Anonymous collective for approximately two months in 2012. Anonymous chatrooms were open access, making it possible for anyone to monitor them and collect data that is made available as timestamp log files. An account was connected to both chatrooms 24/7 and kept all the logs on a daily basis. Conversations took place on an online network called Internet Relay Chat (IRC) where chatrooms allow Internet users to share files, play games, or work with other users, no matter where they are in the world and whether they are in private or public chatrooms. These chatrooms offer the advantage of anonymity through services such as proxies that hide users' IP addresses (Décary-Hétu, Leppänen, 2013).

We focused on two chatrooms during a time where individuals connected with Anonymous Québec were particularly active, analyzing 447 files that contained a total of 21 megabytes of data. The conversations studied consist of 259,668 lines of text. The sixty most active individuals on both chatrooms accounted for, on average, 1,011 messages. If all those who used the chatroom are counted, including people who messaged only once, and the use of pseudonyms is taken into account (a single individual can send a message several times under a particular pseudonym, change to another pseudonym to send other messages, and then return to using the first pseudonym²), the number of most active individuals drops to 41. However, even this reduced number is not representative, as a small number of these individuals were very active, while others seldom participated.

The first chatroom analyzed presented a large amount of information about Anonymous' philosophy and preferred type of attack. The second

² A police officer, affected to the case, was met to help the understanding the use of nicknames and some slang and hacking terms.

chatroom was dedicated to the major operations in Québec during the Maple Spring events and not only provided information about Anonymous's philosophy, choice of targets, and attack techniques but also provided useful information about the context in which they were discussing many topics. The police officer who oversaw the investigation was interviewed on several occasions and provided additional information on technical terms as well as the meaning of certain comments. The investigation report for this case was also consulted. While there were many technical discussions and ask-for-help messages, the focus of this paper has been put on the social aspect of the movement.

4.2 Method

Analysis of conversations was performed using QDA Miner software. This qualitative analysis tool simplifies the processing of a large quantity of texts and made it possible to develop a coding system for vertical analysis of conversations. Each message was coded under a particular theme according to the subject of the conversation³. If participants posted on a particular topic in a continuing conversation, each message was coded. A message could also be coded under more than one topic. For example, part of a conversation could be about a potential target while part was about government corruption. Codes/themes were developed to capture the beliefs and motivations of individuals and specific events, or disputes were coded to allow for a synthesis of events. These steps made it possible to develop a more complete description of events and of the perceptions of individuals in the chatroom.

After the initial coding, we recoded specific topics to identify larger themes that characterized the

discussions. This type of data processing has considerable advantages, including the ability to immerse oneself in the context of that time. Reading and analyzing the daily conversations of particular individuals in the Anonymous movement gave the researchers a chance to see them in their “natural” environment, while conversations between participants contained information that would not have been available through other methods (for example, through a survey). Our method provided an opportunity to access unique and privileged information, essential for the purposes of this work.

5. Results

In this section, we present the important themes that emerged from the analysis of the most prevalent topics discussed, as well as themes that provide insight into the Anonymous movement during the Maple Spring. In analyzing data derived from the chatrooms, five important themes emerged characterized by reoccurring discussions. They discussed the identity of the hacktivist collective, values such as freedom of expression, the media-centric immunity of mass media outlets, their target selection, and the aftermath of the attacks. The themes are explored and described in the following sections, using quotes from the data collected when appropriate.

5.1 Collective Identity

Previous studies have described Anonymous as a movement, a group, and a collective (Mansfield-Devine, 2011; McGovern, Fortin, 2019), demonstrating that there is no consensus on how Anonymous is defined and that discussing the movement's identity requires a great deal of interpretation. This may be due, in part, to the

³ The logs in our sample were bilingual with a majority of messages in French, all text excerpts presented in this paper were translate in English and validated by authors.

decentralized nature of the group, with different definitions provided by different members, who may be influenced by the image of Anonymous depicted in the media. Similarly to that of prior research, our data included several attempts by Anonymous members to describe the movement, which involved both correcting others and justifying the group's existence:

[04:17] <UserA> anonymous doesn't really have any 'rules'.

[04:17] <UserA> just an ideology

[04:21] <UserB> Anonymous is an idea ... a collective consciousness ... but certainly not an ideology

[...]

[10:06] <UserC> anonymous is a group

[16:34] <UserD> we're not a group ...

These excerpts indicate dissent but also show that seldomly a better answer is provided when the description of the group's identity is rejected by others. Anons seem to be providing a personal vision of the group rather than attempting to establish a unified identity for the whole movement. The lack of agreement and lack of negotiation over a particular identity suggests that at least the Anons in this chatroom were not bothered by the lack of a clearly stated collective identity. Other excerpts illustrate that coming up with a strict definition of Anonymous is problematic. Attempts in which the definition is more abstract are generally met with less dissent:

[19:18] <UserE> anonymous it's an idea ... a way of thinkin[g]

[...]

[19:18] <UserF> anonymous its a cyber culture

[...]

[06:22] <UserG> Anonymous is freedom of expression

[...]

[16:45] <UserH> Anonymous is ideas, and people who want to help those ideas.

[...]

[12:19] <UserI> It is a voice for the people that provides the opportunity to speak against what we think is outdated.

As these excerpts illustrate, Anonymous participants see the movement as many things – an idea, a cyberculture, even a voice for the people. Congruent with Coleman's (2020) perspective on Anonymous collective identity, the inclusive and participatory nature of the collective allows for a cohesive identity to exist in a more abstract way than with the collective identity of other movements. There appears to be room for multiple definitions of its identity to coexist within the movement with the condition that they do not create fundamental conflicts. The discussions of identity also suggest that participants have larger goals – a vision in which may be important than the identity of the collective.

5.2 Freedom of Expression

The computer attacks by Anonymous during the Maple Spring were launched in response to Bill 78, the Québec government's attempt to control the student demonstrations that followed their announcement of a tuition increase. Anonymous saw the bill as an attack on citizens' freedom of expression and encouraged Anons to carry out a series of attacks against the government. These

attacks included disabling more than a dozen websites, including those of the Education Department, the Québec liberal party, The Ministry of Public Security of Québec and the Montreal police force as well as publicizing the possibility of online attacks against hotels and guests during the Montreal Grand Prix (Daudens, 2012; Montpetit, 2012). The analysis notes conversations frequently discussed the infringement of students' rights by the Québec government, suggesting that freedom of expression is an essential value for those who identify as Anonymous.

[21:48] <UserS> Anonymous supports freedom of expression

[...]

[10:15] <UserJ> Yeah, but let's remember that the student conflict it not really the subject here, Anon, it's more freedom of expression

It appears that, for some participants, the tuition increase was not the main reason for Anonymous involvement, suggesting a lack of interest in certain types of socio-economic debates. They weren't helping the student movement so much as fighting for individual and collective rights, suppressed by the government. As such, the UserJ's comment highlights how important freedom of expression is for the participants.

Free circulation of information is also among the values defended by participants in the chatrooms. Anonymous has targeted institutions that have attempted to control, limit, or monopolize public information. UserK succinctly summarizes this point:

[16:44] <UserK> We are fighting for freedom of expression in all its forms and without censorship

[...]

[21:07] <UserK> Actions on the Internet = the sole and broad purpose of fighting censorship and defending freedom of expression

We should probably note that censorship as presented above is probably indicative of the limits placed on protestors. It seems that UserK was seeing the limitations as describes in bill 78 was, in a way, censoring the students' messages by limiting protests.

5.3 Immunity of the media

Surprisingly, one topic that surfaced during analysis was that the media must be "protected" or, at the very least, should be immune from target selection. Indeed, not attacking the media seems to be one of their few clearly articulated rules (Olsen, 2012). Discussions suggest that the media should be protected from attacks because they agree with Anonymous about the value of freedom of information, which includes protecting the sources that disseminate such information:

[20:32] <UserL> I am in favor of making the information about failures, faults, leaks, injustice ... etc. as widely [known] as possible.

[...]

[17:05] <UserM> Attacking the media goes against the anonymous idea

[...]

[19:05] <UserN> we don't attack media, anonymous rule

[...]

[17:42] <UserO> if it's censorship, we should give them a message right? ... we don't attack the media ok ... but if it's censorship... it's not the same debate anymore, right?

Several Anons proposed launching attacks on a telecommunication provider and an important TV station, but other individuals quickly pointed out that one of the rules of Anonymous is that the media structure should not be attacked. This rule prompted questions in the chatroom when members realized that some of the media were censoring information.

[17:06] <UserP> and what happens when the media censors the people?

[...]

[16:59] <UserQ> [Telecommunication provider company] controls the pouting people who are little informed ... propaganda, disinformation, censorship, this provider is unworthy of having a news network!!!

Censorship by the media is at odds with Anonymous philosophy, which is based in part on supporting the free flow of information. The comments show that two core values of Anonymous – freedom of information (through the abolition of censorship) and protection of the media, which can be useful in making their activities visible and disseminating their message – were sometimes in conflict. In the end, protecting the media seems to be more important to Anonymous than their desire to fight censorship, as no hacking acts targeting any media outlets were recorded.

One possible hypothesis which could explain the importance of traditional media is that Anonymous depends on the media in fulfilling their goal: an attack that is presented in the media is seen as a proof of a successful attack, as it gives the movement greater impact on the political level by reaching the general population rather than just members. For example, UserTT reported to the group that their promotional video had been shown by a TV news station.

[14:33] <UserTT> our video is now playing on [TV news station]

[14:33] <UserTT> Victory!

For Anons, dissemination of their work in the media is an important reward as it provides them with a wider audience for their message and also creates a sense of belonging and excitement among participants in the movement.

5.4 Target Selection

Target selection was a recurring topic of discussion in the chatrooms and there were many brainstorming sessions of variable lengths. These sessions were characterized by conversations about ideas for potential targets, sometimes in response to current events.

[12:07:28] <UserR > Why not attack the government server?

[...]

[12:14:50] <UserR> Would you attack all government sites (and including AFE [the Student Financial Aid Service of Quebec]) or just some government sites?

[...]

[14:12] <UserS> Should we first decide on the target for a new attack: [prime minister], [minister of education], or [name of a popular event in Montreal]?

[...]

[18:41] <UserRR> It is necessary to attack good targets to send the right message

The process of selecting a target in the chatrooms seemed to be that hackers would suggest a good potential target to other users, who would then offer their opinions. The term “good target” was commonly used to designate a target that is in line with the philosophy and values of the movement (i.e., launching computer attacks to defend values such as freedom of expression and freedom of information) by targeting those they believe were contravening individual and collective freedoms. As mentioned in the previous excerpts, it was frequently observed that Anons were against the actions of the ruling political party at the time, making proposals to attack government websites an obvious “good target” to Anons in the chats. The opinions of other participants in the chatroom were solicited and some form of acknowledgement was sought before taking action. After discussion and informal approval, participants seem to reach a consensus on their next target fairly quickly:

[12:09:42] <UserT> Okay What's the attack today?

[12:09:45] <UserU> [police dept.] is a good target

[12:09:56] <UserV> I would say [police dept.]

[12:10:30] <UserV> Same tactic for weeks, they don't want to try anything. [police dept.] must go down.

[...]

[12:09:40] <UserW> Okay, what about the [opposition political party] then?

[12:09:43] <UserX> it's a good target

[12:09:58] <UserY> it's true

While participants provided opinions about which target should be selected and why, certain emotional responses to the events were observed to impact the selection of certain targets, particularly, when government entities were the subject of the discussion:

[21:08] < UserWA> fuck law 78

[21:08] < UserX > That's why it must be dropped

[18:56] <UserYQ> [UserED], anonymous is a symbol, we prove to the world that we can attack the government

[18:56] <UserYC> and the government is attacking the people

[...]

[09:33] < UserY> that we let a rotten government ... tell us what to do and what not to do ... disgust Ccharest and acolytes of this world that believes itself themselves gods when they are nothing more than worms

[10:52] <UserXA> I wish someone would take down the canadian conservative party website. Yesterday #DenounceHarper was trending on twitter, I was so happy

[17:09] < UserQRT> anyway... it's not the media [that's] the problem

[17:09] < UserQRT> it's government

The quoted excerpts suggest that Anonymous participants were consistent in carrying out their attacks according to an underlying ideological cause

and in defending the collective values of the movement even when emotions such as anger were present. However, when we compared these collective values with the individual values expressed by some chatroom users, we observed some discrepancies: some individuals proposed targets that were not related to the movement or carried out attacks without consulting others in the chat room:

[19:03] <UserV> HACKED [Municipality A - adjacent to Montreal site URL]
[19:04] <UserZ> Seriously... why [[Municipality A]]?
[19:05] <UserAA> [[Municipality A]] is a seriously bad target

By hacking into a municipality's website, rather than into targets that fit the group's philosophy, this user created a conflict between his/her actions and Anonymous principles. The interventions and actions suggest that he/she might have been hacking out of excitement rather than as a protest. Such cases were not common but illustrates that the personal values of some individuals occasionally clashed with the collective values of the movement.

[23:08] <UserBB> No one understands why [[Municipality B]] was targeted even we don't understand
[...]
[14:25] <UserCC> Yesterday I hacked into a holiday camp site, the camp [name of the summer camp] xD joy!
[14:26] <UserDD> Who cares?
[14:26] <UserEE> I hope you're not proud of it

[14:28] <UserFF> Yeah, it's not great ...
[...]
[12:20] <UserRR> we should all attack FB for no particular reason >_>

It should be noted that Municipality B was located in the north part of the province and there was no obvious link to the events. Also, Facebook was also suggested as a target, despite UserRR's clear indication that attacking Facebook was not a part of the Maple Spring events, suggesting that the motivations of some participants may be incongruent with the general objectives of the Anonymous chatroom.

5.5 Reception and Perception of the Aftermath of Attacks

In the chatrooms, a few individuals posted about how they had managed to break into various unidentified systems, obtained personal information about police officers, government officials, or consumers, and then disseminated this information. Some mentioned that they had hacked into the servers of the Québec National Institute for Public Health (*Institute National de Santé Publique du Québec* (INSPQ)) and the Montreal Police Service (*Service de Police de la Ville de Montréal* (SPVM)). Anons were proud of their successes and happy to share them. A collective sense of joy and pride was visible in the chatroom after a success was reported through the use of emoticons (xD, :D) which illustrate a sideways smiley face indicative of happiness/joy.

[20:47] <UserCC> I AM ENTERING IN <http://www.inspq.qc.ca>
[20:48] <UserCC> and I AM AMDIN
[...]
[21:03] <UserCC> I AM IN SERVER xD

[21:03] <UserQQ> How did you do all this with cmd

[21:04] <UserRR > Are you telling me that you are in the spvm server?

[21:04] <UserSS> I have all the files on the server: D

In addition to reporting intrusions into unidentified servers, participants claimed they had obtained information about the identities and banking data of ticket buyers for a popular event in Montreal, had identified clients of a bank that had many police officers as clients, and had obtained contact information for senior executives of a police department. It was not possible to confirm whether the intrusions and dissemination of confidential information boasted about in chatrooms had actually occurred. While the government website hacks discussed in the chatrooms were reported in the media; such as in the *Toronto sun*, the *Globe and Mail* and *Radio-Canada*, (Daudens, 2012; Montpetit, 2012; QMI Agency, 2012), others may have been invented to gain recognition from those in the chatroom.

6. Discussion

The present study describes the topics that were discussed in Anonymous' chatrooms during Maple Spring. While some studies (Kelly, 2012) argue that collective identity is important in creating a cohesive membership and helping determine the identity of individual members, others suggest that collective identity is often only the acknowledgement of a shared willingness to fight for a common cause rather than the embodiment of a particular identity held by members (Bennett, 2005). For Anonymous, how each member defines the group appears to be less important than the opportunities it provides for

positive interactions with other members. Social movements are often formed not by individuals who identify only with a single group but by those who identify with various groups, creating a mosaic of protest identities operating under a single banner (Treré, 2015). This benefits groups such as Anonymous because, as participants are able to create their own meanings within a broad collective, the group as a whole is not limited to the types of campaigns in which it can engage (Machado, 2015). It is this fluidity and collection of coexisting identities which allow Anonymous to continue to organize, contrary to the characterisation of Anonymous as ineffective and rife with dissent (Caldwell, 2015; Kelly, 2012). Both the literature and our data support the view that Anonymous does not have one collective identity but rather collective identities, created through positive communication, particularly within the chat rooms. The excerpts have shown that the movement can encompass its values (through userG), its goals (UserH) its ability for change (UserI) and other abstract features. Given the number of cyberattacks undertaken but those on the chat during the Maple Spring, it seems the ways in which members define the group's identity is of little consequence in practice, having demonstrated their ability to carry out hacking operations. This seems more like a simple exercise than a fundamental requirement for participation.

An analysis of conversations between Anonymous members suggests that the philosophy of the hackers at this time was based on few, generally accepted, values. The emphasis on freedom of expression extracted from our data is in line with that of previous studies which suggest that freedom of expression is a central value for Anonymous members (Ludlow, 2010). The conversations

analyzed also demonstrate an interplay between ideas of freedom of expression, freedom of speech, and freedom of information, to which members sometimes seem to see as overlapping. This made it difficult to discern nuanced distinctions between said concepts presented by those using the chatroom. While students began their demonstrations as protesting tuition hikes, Anonymous only mobilized once Bill 78 was introduced, an act they saw as a limitation on protestors' freedom of expression. This mobilization was consistent with other actions by Anonymous, which have targeted traditional institutions of power that attempt to limit freedom of expression (Mansfield-Devine, 2011).

Our study highlights the importance of the media to the hackers as well. As mentioned earlier, suggestions targeting the media were easily ruled out, particularly those that suggested attacks on traditional media (media outlets). Anons in the chatrooms seemed to agree that traditional media should be protected and any dissent over this position was quickly and forcibly shut down, although this did not stop Anons from criticizing the media and questioning the role of telecommunication company providers and the control they have over the media. Participants in the chatrooms seemed aware that the concepts of freedom of information and censorship were closely linked. It must be noted, however, that other campaigns contradict this interpretation, as media outlets under state control have been the target of cyberattacks. RT, a Russian state-sponsored media outlet was hacked during the early weeks of the Ukrainian invasion (Bonifacic, 2022). In this case, it can be suggested that the media outlets are not operating under a value of freedom of information, but an agent of the state, such as police forces,

pushing government propaganda and misleading citizens. It is not surprising that Anonymous aligns those media outlets as another arm of government repression.

Protecting the media suggests that those in the chatrooms recognize that traditional media acts as a third-party broker between Anonymous and the public and any attack on the media could affect Anonymous's public image. As the movement is a political entity, the opinion of the general public matters. Losing public approval could have devastating implications for Anonymous, delegitimizing their campaigns, their actions, and their general cause. Another possibility is that Anons recognize the greater need for traditional media to spread their message to a larger audience. The conversations analyzed in our study show that Anonymous's goal is to use electronic civil disobedience techniques to denounce those who attempt to stifle freedom of expression. Such acts work best when they are disseminated to a large audience, encouraging the public to hold a particular opinion about the transgressor. This reflection among participants in the chat room is indicative of the importance of assertion, as described by George and Leidner (2019), even though these participants may not be involved in the social media aspect. While Anonymous discusses successful campaigns on their social media pages, these publications reach only those who follow Anonymous, many of whom presumably already support their message. Recognizing that the media is key to publicizing their actions to a wider audience suggests that Anonymous is aware that denouncing transgressors is most effective if the denunciation reaches the socio-political sphere, making everyday people aware of the abuses committed by traditional institutions of power.

The reaction to events carried out by Anonymous also demonstrated the importance of the media as an indicator of success. Anons in the chatrooms were excited about announcing that their actions had been mentioned on the news, because it meant that they had reached a larger audience. Recognition in the media validates actions against a chosen target, providing tangible proof of a successful operation and leading to validation from other members, as well as indicates a greater socio-political impact of an attack outside of solely the group and its targets. Anons celebrated news broadcasts about a successful operation, creating positive interactions between members. As Treré (2015) suggests, such interactions are important for a collective unity among members. While the individual motivations of each Anon in the chatroom cannot be determined, the data show that a successful operation had the secondary effect of promoting continued identification with other Anonymous members when the success was celebrated in the same chatrooms where targets had been selected.

Regarding consensus on target selection, few arguments or pushbacks were observed, demonstrating a sense of teamwork between Anons online. There seemed to be informal leaders who dominated the conversation and proposed potential targets, in line with the descriptions of the group by Coleman (2014) and Mansfield-Devine (2011). Two types of targets were observed in the present study: targets that were unanimously agreed upon good and bad targets. The good targets proposed in the chatrooms were largely traditional institutions of power: government, police, and political parties. Anonymous has focused on such targets in the past, which may explain why consensus was so easily reached (see Thackray, McAlaney, 2018). Proposing

traditionally “safe” targets that are likely to incite positive reactions from other Anons also ensures positive interactions between members (Treré, 2015). Suggested targets that were quickly denounced included a children’s camp, municipal governments, and the media. Those who proposed targets that were rejected were apparently either unaware that the proposed targets were considered out of bounds by the group or were motivated by individual interests (e.g.: for fun, the need to prove themselves, etc.). The instances of bad targets being attacked without the approval of others in the chatrooms, suggested that bad targets are considered those in which an attack would not send the appropriate message. This demonstrates that hacking is not the finality, but that target selection process is about sending the right message based on the same Anonymous values as those on social media. For that reason, targets such as distant municipalities and summer camps were considered outside the context of fighting for freedom of expression, and therefore a bad target.

There are a couple of limitations to this study that should be addressed. Its results are congruent with a decade of recent research arguing Anonymous, cyberattack targets are infringing on individual freedom of expression and social issues (Bardeau, Danet, 2011; Beran, 2020; Coleman, 2020; Ludlow, 2010). Regardless, in order to validate the results of the present study, an analysis of multiple target selection conversations among multiple Anonymous campaigns is needed. Future research should attempt to diversify the sampled population to achieve a greater level of generalisability. We also found that much of the conversation was dominated by a few participants. This affects the results as the largest number of Anons in the chatrooms took a more observational role, rarely

engaging in conversation. Results might have been different had all the participants participated equally. While this may not have had an effect on the values of the group, it might have affected the target selection process in particular, as it can be assumed that the more people engage in a discussion, the greater the chance of miscommunication and debate. Greater discussion could also demonstrate a wider variety of targets proposed which could have shown how other members in the chat rooms deal with targets that are not traditionally good targets frequently chosen by Anons.

7. Conclusion

The present study argues that Anonymous values have remained steady over the course of a dozen years in both the hacker and social media contingents of the group. The few values Anonymous members hold, particularly freedom of expression, freedom of speech and freedom of information are held in high regard and include rules as infallible values during the target selection process (particularly traditional media's immunity). Most notably, the media's importance cannot be understated, as it acts as a third-party broker between Anonymous's message and the general public. While more recent hacks against Russian TV would suggest otherwise, the context to which the media in Russia exists reinforces the impunity of the media (Bonifacic, 2022). The media itself is not protected, but for the freedoms of expression and information it represents. With the inclusion of social media for assertion, traditional forms of media are no longer the sole gatekeeper for wider audiences. Thusly, the media remains immune to cyberattacks so long as it remains an active proponent of these freedoms. This suggests the target selection process of future campaign will

continue to evaluate the media's involvement and relationship to the state, as to ensure it reinforces the same values as the collective. As Operation Russia indicates, any deviation for the promotion of freedom of information can make a bad target a suitable target for cyberattacks.

The media also acts as a barometer for successful operations, as it shows proof of an attack having taken place, which in turn offers Anons the opportunity to gloat, feel joy, and interact positively with one another. Possibly, due to the search for positive interactions among members, which may explain why we observed mainly traditional Anonymous targets being suggested as suitable targets. Contrary to literature suggesting Anonymous is characterised by confusion or infighting amongst members, Anonymous seemingly thrives on a lack of identity, or rather, a collection of multiple personal identities to co-exist. These findings must remain in the context of both space and time, as 2012 is now in the past. However, Anonymous has mounted many similar campaigns; most recently in 2020, against U.S. police forces and 2022, against the Russian government, as proof of Anonymous' continued relevance (Everington, 2022; Franceschi-Bicchierai, 2020). For this reason, research must continue to analyse and understand this unique and impactful form of social activism.

References

1. Auty C., «Political Hacktivism: Tool of the Underdog or Scourge of Cyberspace?», *Aslib Proceeding*, vol. 56, issue 4, 2004, pp. 212-221.
2. Bardeau F., Danet N., *Anonymous : Pirates informatiques ou altermondialistes numériques ? : Peuvent-ils changer le monde ?* Éditions FYP, 2011.

3. Bégin-Caouette O., Jones G., «Student organizations in Canada and Quebec's "Maple Spring"», *Studies in Higher Education*, vol. 39, 2014, pp. 412-425.
4. Bennett L., «Social Movements Beyond Borders: Organization, Communication, and Political Capacity in two Eras of Transnational Activism», *Transnational Protest and Global Activism*, 2005, pp. 203-226.
5. Beraldo D., «Unfolding #Anonymous on Twitter: The Networks Behind the Mask», *First Monday*, vol. 27, n. 1, 2022.
6. Bergeron A., Delle Donne J., Fortin F., «Une Publication pour Dénoncer, Sans Plus : Description des Activités des Groupes Facebook S'identifiant au Mouvement Anonymous au Canada», *La Criminologie de L'information : État des Lieux et Perspectives*, vol. 52, n. 2, 2019, pp. 35-62.
7. Beyer, J., *Expect Us: Online Communities and Political Mobilization*, Oxford University Press, New York, 2014.
8. Bodó, B., «Hacktivism 1-2-3: How Privacy Enhancing Technologies Change the Face of Anonymous Hacktivism», *Internet Policy Review*, vol. 3, n. 4, 2014, pp. 1-13.
9. Caldwell T., «Hacktivism goes hardcore», *Network Security*, vol. 5, 2015, pp. 12-17.
10. Coleman, E. G., «Logics and Legacy of Anonymous», in Hunsinger, J., Allen, M., Klastrup, M., (Eds.), *Second International Handbook of Internet Research*, Springer, 2020, pp. 145-166.
11. Coleman, E. G., «Hacker politics and publics», *Public Culture*, vol. 23, n. 3, 2011, pp. 511-516.
12. Coleman, E. G., *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, Verso, 2014.
13. Conway, M., «Hackers as terrorists? Why it doesn't compute», *Computer Fraud and Security*, vol. 12, 2003, pp. 10-13.
14. Décary-Héту D., Leppänen A., «Criminals and Signals: An assessment of criminal performance in the carding underworld», *Security*, vol. 29, n. 3, 2013, pp. 442-460.
15. Denning D. E., «Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy», in Arquilla, J., Ronfeldt, D., (Eds.), *Networks and netwars: The future of terror, crime, and militancy*, RAND, 2001, pp. 239-288.
16. George J. J., Leidner D. E., «From Clicktivism to Hacktivism: Understanding Digital Activism», *Information and Organization*, vol. 29, n. 3, 2019, pp. 1-45.
17. Guiton A., *Hackers : Au Cœur de la Résistance Numérique*, Éditions Au diable Vauvert, 2013.
18. Gunkel D. J., «Editorial: Introduction to hacking and hacktivism», *New Media & Society*, vol. 7, n. 5, 2005, pp. 595-597.
19. Hampson N. C. N., «Hacktivism: A New Breed of Protest in a Networked World», *Boston College International and Comparative Law Review*, vol. 35, n. 2, 2012, pp. 511-542. <https://heinonline.org/HOL/P?h=hein.journals/bcic35&i=515>
20. Jones K., Nurse J. R. C., Li S., «Behind the Mask: A Computational Study of Anonymous' Presence on Twitter», *Proceedings of the Fourteenth International AAAI Conference on Web and Social Media (ICWSM 2020)*, vol. 14, 2020, pp. 327-338.
21. Jones K., Nurse J. R. C., Li S., «Out of the Shadows: Analyzing Anonymous' Twitter Resurgence during the 2020 Black Lives Matter Protests», *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 16, 2022, pp. 417-428.
22. Kahn R., Kellner D., «New Media and Internet Activism: From the 'Battle of Seattle' to Blogging», *New Media & Society*, vol. 6, n. 1, 2004, pp. 87-95.
23. Karatzogianni, A., *Hackers during cyber conflict. Violence and war in culture and the media. Five disciplinary lenses*, Routledge, New York, 2013.
24. Kelly B. B., «Investing in a Centralized Cybersecurity Infrastructure: Why Hacktivism Can and Should Influence Cybersecurity Reform Note», *Boston University Law Review*, vol. 92, n. 5, 2012, pp. 1663-1712.
25. Kenney M., «Cyber-Terrorism in a Post-Stuxnet World», *Orbis*, vol. 59, 2015, pp. 111-128.
26. Li X., «Hacktivism and the first amendment: Drawing the line between

- cyber protests and crime», *Harvard Journal of Law & Technology*, vol. 27, issue 1, 2013, pp. 302-329.
27. Ludlow P., «WikiLeaks and Hacktivist Culture», *The Nation*, vol. 4, 2010, pp. 25-26.
 28. Machado M. B., «Between Control and Hacker Activism: The Political Actions of Anonymous Brazil», *Historia, Ciencias, Saude—Manguinhos*, vol. 22, 2015, pp. 1531-1549.
 29. Manion M., Goodrum A., «The Ethics of Hacktivism», *Journal of Information Ethics, suppl. Special Issue: New Challenges to Ethics and Law; Jefferson*, vol. 9, n. 2, 2000, pp. 51-59.
 30. Mansfield-Devine S., «Anonymous: Serious Threat or Mere Annoyance?», *Network Security*, vol. 1, 2011, pp. 4-10.
 31. McCrow-Young A., Mortensen M., «Countering Spectacles of Fear: Anonymous' Meme War' Against ISIS», *European Journal of Cultural Studies*, vol. 24, n. 4, 2021, pp. 832-849.
 32. McGovern V., Fortin F., «The Anonymous Collective: Operations and Gender Differences», *Women & Criminal Justice*, vol. 30, n. 2, 2019, p. 1-15.
 33. McKelvey F., «Digital Media and Democracy Tactics in Hard Times», *Canadian Journal of Communication*, vol. 35, n. 2, 2010.
 34. Pendergrass W. S., «What is anonymous? A case study of an information systems hacker activist collective movement», [Doctoral Dissertation], Robert Morris University, 2013.
 35. Raynauld V., Lalancette M., Tourigny-Koné S., «Political Protest 2.0: Social Media and the 2012 Student Strike in the Province of Quebec, Canada», *French Politics*, vol. 14, n. 1, 2016, pp. 1-29.
 36. Renzi A., «Info-capitalism and resistance: How information shapes social movements», *Interface: A Journal for and about Social Movements*, vol. 7, issue 2, 2015, pp. 98-119.
 37. Romagna M., «Hacktivism: Conceptualization, Techniques, and Historical View», *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, pp. 743-769.
 38. Thackray H., McAlaney J., «Groups Online: Hacktivism and Social Protest», in McAlaney J., Frumkin L. A., Benson V. (Eds.), *Psychological and Behavioral Examinations in Cyber Security*, IGI Global, Hershey, 2018, pp. 194-209.
 39. Treré, E., «Reclaiming, Proclaiming, and Maintaining collective identity in the #YoSoy132 movement in Mexico: An examination of digital frontstage and backstage activism through social media and instant messaging platforms», *Information, Communication & Society*, vol. 18, n. 8, 2015, pp. 901-915.
 40. West, S. M., *Ambivalence in the (Private) Public Sphere: How Global Digital Activists Navigate Risk*. 7th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 17), 2017.

Sitography

1. AFP, «Canada: Hackers Targeted Country's 2015 Election, May Try Again», *SecurityWeek.Com*, 2017, June 18, [News Media], available on the internet site: <https://www.securityweek.com/canada-hackers-targeted-countrys-2015-election-may-try-again>
2. Anderson N., «“Literally” the day he was arrested, hacker “Sabu” helped the FBI», *Ars Technica*, 2012, May 4, [News Blog], available on the internet site: <https://arstechnica.com/tech-policy/news/2012/05/literally-the-day-of-his-arrest-hacker-sabu-helped-the-fbi-ars>
3. Beran D., «The Return of Anonymous», *The Atlantic*, 2020, August 11, [News Blog], available on the internet site: <https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/>
4. Bonifacic I., «Anonymous claims responsibility for Russian government website outages», *Yaboo!Finance*, 2022, February 26, [News Blog], available on the internet site:

- <https://finance.yahoo.com/news/anonymous-hacks-russia-websites-190045299.html>
5. Canadian Centre for Cyber Security, *Cyber Threats to Canada's Democratic Process*, 2018, [Report], available on the internet site: <https://cyber.gc.ca/en/>
 6. Castrodale J., «Hackers Jammed Chicago Police Scanners With Internet Classic “Chocolate Rain”», *Vice*, 2020, June 1, [Blog], available on the internet site: https://www.vice.com/en_us/article/889nw4/hackers-jammed-chicago-police-scanners-with-internet-classic-chocolate-rain
 7. Daudens, F., «Les Anonymous piratent plusieurs sites du gouvernement du Québec», *Radio Canada*, 2012, May 21, [Blog], available on the internet site: <https://web.archive.org/web/20130822085752/http://blogues.radio-canada.ca/surleweb/2012/05/21/anonymous-operation-quebec/>
 8. de la Hamaide, S., «Timeline of Paris Attacks According to Public Prosecutor», *Reuters*, 2015, November 14, [News Media], available on the internet site: <https://www.reuters.com/article/us-france-shooting-timeline/idUSKCN0T31BS20151114>
 9. Everington, K., «Anonymous hacks into Russian firm running Ukrainian nuclear plants», *Taiwan News*, 2022, March 15, [News Media], available on the internet site: <https://www.taiwannews.com.tw/en/news/4474025>
 10. Faïfe, C., «Anonymous-linked group hacks Russian space research site, claims to leak mission files», *The Verge*, 2022, March 3, [News Blog], available on the internet site: <https://www.theverge.com/2022/3/3/22960183/anonymous-hack-russian-space-research-roskosmos-ukraine>
 11. Franceschi-Bicchierai, L., «“Anonymous” Is Going Viral Again, But Is It Really Back?», *Vice*, 2020, June 1, [Blog], available on the internet site: https://www.vice.com/en_us/article/wxq5mm/anonymous-minneapolis-george-floyd-protests
 12. Jul C., «Hacktivism & Anonymous», *Calum Stuart*, 2013, July 30, [News Blog], available on the internet site: <http://calumstuart.com/hacktivism-anonymous/>
 13. Kika T., «Anonymous hacks into Russian printers to deliver resistance information», *Newsweek*, 2022, March 21, [News Media], available on the internet site: <https://www.newsweek.com/anonymous-hacks-russian-printers-deliver-resistance-information-1690269>
 14. Levesque C., «Grève Étudiante : Un vidéo d'Anonymous dénonce la loi 78 et lance l'Opération Québec», *HuffPost Québec*, 2012, May 20, [News Media], available on the internet site: https://quebec.huffingtonpost.ca/2012/05/20/anonymous-operation-quebec_n_1531489.html
 15. MacLellan S., «Canada's Voting System Isn't Immune to Interference», *Centre for International Governance Innovation*, 2018, November 5. [News Media], available on the internet site: <https://www.cigionline.org/articles/canada-s-voting-system-isnt-immune-interference>
 16. Molloy D., Tidy J., «George Floyd: Anonymous hackers re-emerge amid US unrest», *BBC News*, 2020, June 1, [News Media], available on the internet site: <https://www.bbc.com/news/technology-52879000>
 17. Montpetit J., «Anonymous hacking campaign in Quebec draws attention of Montreal police», *The Globe and Mail*, 2012, May 31, [News Media], available on the internet site: <https://www.theglobeandmail.com/news-national/anonymous-hacking-campaign-in-quebec-draws-attention-of-montreal-police/article4224869/>
 18. Papadopoulos L., «Anonymous says Russia's spy satellites are now hacked. But the nation denies everything», *Interesting Engineering*, 2022, March 3, [News Blog], available on the internet site: <https://interestingengineering.com/says-russia-denies-anonymous-hack-claims>

19. Purtill J., «Anonymous takes down Kremlin, Russian-controlled media site in cyber attacks», *ABC News*, 2022, February 24, [News Media], available on the internet site:
<https://www.abc.net.au/news/science/2022-02-25/hacker-collective-anonymous-declares-cyber-war-against-russia/100861160>
20. QMI Agency, «Quebec Liberal, government sites hacked», *Toronto Sun*, 2012, May 19, [News Media], available on the internet site:
<https://torontosun.com/2012/05/19/quebec-liberal-government-sites-hacked>