European Journal of Sustainable Development (2020), **9**, 4, 295-302 ISSN: 2239-5938
Doi: 10.14207/ejsd.2020.v9n4p295

Forms and Consequences of the Cyber Threats and Extortion Phenomenon

By Ioana Vasiu[1], Lucian Vasiu[2]

Abstract
Cyber threats and extortionate communications usually aim to influence the behavior or obtain compliance from victims. The phenomenon includes a wide range of forms, such as intimate partner violence; violence against women; dating abuse; sexual harassment; sexual coercion and extortion; etc. The victimization is linked to personal insecurity or disruption, mental and physical health, work or school performance, may represent a high financial burden, affecting negatively the sustainable development in a number of ways. The scale, scope, and challenges posed by this criminal phenomenon cannot be overstated. A deep analysis of the nature and extent of cyber extortion and threat is an essential component in the design of control strategies and programs. This research aims to provide an in-depth examination of the cyber threats and extortion phenomenon. The approach is interdisciplinary and empirically-informed. The analysis was done on a large number of cases and provides a comprehensive description of the essential characteristics of the phenomenon, including forms, communication vectors, and consequences for victims. The article concludes with recommendations for effectively addressing the phenomenon.

Keywords: Cybercrime, Extortion, Speech, Threats, Violence, Discrimination, Ransomware

1. Introduction

Socio-cultural factors affect the thoughts and actions of people and, consequently, substantially impact sustainable development. These factors can be significantly influenced by the use of information and communication technology (ICT), which has the capacity to greatly increase connections and expand the communication opportunities. However, alongside numerous benefits, the use of ICT spawns noxious side effects, such as opportunities and a massive scope for cyberviolence.
Cyberviolence can be defined as the use of information systems to "cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities" (Cybercrime Convention Committee, 2018: 5). Cyberviolence takes numerous forms and is globally regarded as a problem that poses significant socio-cultural and economic challenges, that must to be effectively addressed (Women and Gender Equality Canada, 2019; van der Wilk, 2018; European Institute for Gender Equality, 2017).
Cyber threat and cyber extortion are two prominent examples of cyberviolence. These are acts of "conditional speech intended to influence or gain compliance from a target recipient" (Spitzberg & Gawron, 2016: 47) and present a number of attributes, such as intentionality, harm or undesirable consequences, preferred outcome, contingency,

[1]Prof. Dr., Faculty of Law, Babeş-Bolyai University. Corresponding Author
[2]Ph.D., MBA, Computer Scientist, Expert in Information Systems Security and Cybercrime Prevention

credibility, and likelihood. Extortionate and threatening communications can be instrumental in gaining the "feeling of power and control" (U.S. v. Killen, 2018) over victims through intimidation, isolation, and control (Eisenberg, 2015).

Threatening and extortionate communications amount to direct violations of fundamental human rights, principles of liberty and safety, and, in general, social-cultural sustainability. Even though the actual prevalence of these is not known, these offenses, unquestionable, represent a major concern, at individual and society levels.

The prohibition of true threats "protect[s] individuals from the fear of violence" and "from the disruption that fear engenders," in addition to protecting people "from the possibility that the threatened violence will occur" (RAV v. St. Paul, 1992: 388). Moreover, the control of this phenomenon helps promote important Development Goals, set by the United Nations, such as the advancing gender equality (Goal 5), the inclusive and sustainable economic growth, employment, and decent work for all (Goal 8), and justice, so that people would be free of fear from all forms of violence, whatever their "ethnicity, faith or sexual orientation" (Goal 16) (United Nations, 2015).

An essential component in the design of prevention and control strategies, policies, and programs is a deep analysis of the nature and consequences of the phenomenon. This article is a comprehensive inquiry into the phenomenon and aims to present the forms of the cyber threats and extortion communications and to analyze the main attributes of the phenomenon.

The research approach is interdisciplinary and empirically-informed. The analysis was done on a large number of cases, brought to U.S. Courts, discussed in the academic literature, or reported in law enforcement press releases or assessments. The research method involved a multi-step process, consisting of content analysis, identification of the most important conceptual aspects and characteristics of the phenomenon, categorization, and analysis of these elements.

2. Conceptual Issues and Characteristics of the Phenomenon

2.1 Introductory Remarks

Free speech is an important human right, however, there are several categories of unprotected speech, such as the incitement to lawless action, the communication of true threats, and the speech integral to criminal conduct (Volokh, 2016; Harawa, 2014).

A "threat" can be defined as "an avowed present determination or intent to injure presently or in the future" (U.S. v. Alkhabaz, 1997: 1502). "True threats" are serious threats, "distinguished from mere political argument, idle talk, or jest," a "declaration of intention, purpose, design, goal, or determination to inflict punishment, loss, or pain on another, or to injure another or his property by the commission of some unlawful act" (U.S. v. Twitty, 2019), or a "serious statement expressing an intention to do an act which under the circumstances would cause apprehension in a reasonable person, as distinguished from idle or careless talk, exaggeration, or something said in a careless manner" (U.S. v. Parr, 2008: 497).

The phenomenon encompasses numerous, often severe, such as intimate partner violence (IPV), characterized by emotional, physical, or sexual violence, actual or threatened); cyber dating abuse (CDA); violence against women and girls (VAWG); etc.

Moreover, threatening communications can be a precursor to potentially aggressive and dangerous physical violence, such as physical assault or even murder.
Threatening communications may cause severe effects on the victims, such as personal safety concerns and, in particularly disquieting cases, major adverse health effects, such as anxiety attacks (U.S. v. Humphries, 2013).

2.2 Threats

Threatening communications are used for several reasons. According to researchers, one of the main reasons is "to confront people with the consequences of a behavior" (Peters, Ruiter, & Kok, 2014: 77), with a view to change it.
Threatening communications can be interpersonal and impersonal. The former category encompasses cases of direct relations, in a number of settings, usually transmitted with a view to obtain compliance in a relationship. The latter category includes cases that target leaders or groups of people (for instance, law enforcement, ethnic, minority, etc.) (U.S. v. Davis, 2020; U.S. v. Jordan, 2017).
Threats are often communicated in situations discerned as coercive, perturbing, or distressful, usually determined by economic and/or social pressures. Threats can be also classified as reactive, as response to real or perceived events or threats (for instance, retaliation for loss of job), and proactive, as a perceived way to achieve certain goals (in an attempt to make certain expectations or aspirations become reality) (U.S. v. Swarbrick, 2018). For example, offenders aim to obstruct justice, to prevent access to abortion services, to block certain forms of activism, etc. There are, however, cases where the offenders inflict fear for their own gratification or enjoyment (U.S. v. Haileselassie, 2019).
The typical offenders present significant concerning issues, such as low self-control or impulsivity; depression; psychopathic and Machiavellian traits; sensitivity to criticism; hostility; angriness; mental disorders; cognitive capabilities lower than the general population; and limited capacity to empathize (Peterson & Densley, 2017; Warren, Ogloff & Mullen, 2013; Leary, Twenge, & Quinlivan, 2006).
Cyber threats usually aim to influence the recipient, to obtain compliance with certain demands, rather than actually engaging on the course of action described. However, threats do have a composite relationship to actual harm.
Speech can cause harm as it may influences the receiver of the communication to react in a certain way. Speech can inflict "psychological harm on the listener in the direct manner that a physical attack would inflict physical harm" (Han, 2014: 1659). Moreover, the harm "may be real whether or not the individual speaker intended his speech to be received as a threat, and regardless of whether the speaker actually intended to carry out such a threat" (Romney, 2012: 639).
A number of cyber communication characteristics also increase the challenges posed by the phenomenon. For instance, it is difficult to infer offenders actual state of mind and whether those making the threats are actually capable to carry out the threats communicated. Further, technology allows the communication of threats using the identity of another person (U.S. v. Turrella, 2012) or multiple-identities (U.S. v. Whitmore, 2019), and to reach a large number of people, potentially amplifying the fear, anxiety, or terror (U.S. v. Bishop, 2018).
Even more concerning, there can be anti-social threats, communicated in anonymous

ways (U.S. v. Bagdasarian, 2011), that may reach followers or viewers, which, in turn, may, potentially, be willing or encouraged and capable to fulfill the spur for violent actions, effectively triggering a contagion effect. Such threats are widely acknowledged as significant risk indicators of potentially violent, criminal, or even terrorist behavior.

To accomplish their objectives, the offenders use a variety of threats, such as to disclose extramarital affairs; to post damaging information; to injure the property, the reputation, or the person of another; even to kill. Threatening communications may include disturbing or obscene images; graphic invectives; negative comments on victim's health, habits, or looks; incitement to discrimination or violence against persons or groups of people; etc.

The language employed can be unambiguous, implied, veiled, or somewhat cryptically. In a number of cases, the language used is truly sadistic. For illustration, in U.S. v. Wheeler (2019), the defendant threatened to "kill cops[,] drown them in the blood of thier [sic] children, hunt them down and kill their entire bloodlines"; in U.S. v. Cain (2018), the defendant, in heinous terms, threatened to kill his ex-wife's mother, ex-wife and her new boyfriend, to send to members of victim's family videotapes showing the victim engaged in sexual acts, and to rape victim's daughter; in U.S. v. Heineman (2014: 972), the defendant, sympathizer of the white supremacy ideology, sent to the victim e-mails containing very reprehensible statements, such as "slay you, by a bowie knife shoved up into the skull from your pig chin you choke, with blood flooding in your filthily treasonous throat!"); in U.S. v. Williams (2018), the defendant threatened to kill a judge, "sodomize the corpse, into pieces, and mail one piece of the corpse to the courthouse each week"; in U.S. v. Vandevere (2019), the defendant transmitted a picture depicting a lynching; etc.

Threatening communications use numerous vectors: e-mail; online call spoofing services; SNS; etc. A number of cases illustrate the use of SNS: in U.S. v. Michael (2012), for instance, the defendant posted on Facebook threats to "kidnap and injure DEA agents and personnel" and "time we answered their crimes with bloodshed and torture"; in Commonwealth v. Knox (2018: 1149), the appellant recorded and uploaded to YouTube a rap song titled "F--k the Police," with lyrics that contained "descriptions of killing police informants and police officers." The intensity of the threats can be increased by repeated communication and by the use of multiple vectors, such as Facebook, e-mail, and telephone (U.S. v. Leach, 2017).

2.3 Extortionate Threats

The term "extortion" encompasses numerous forms. The Florida law definition, for instance, includes, among other things, the use of threats to injure a person's reputation, to expose another to disgrace, or to reveal "any secret affecting another" for the purpose of compelling the victim "to do any act or refrain from doing any act against his or her will" (Fla. Stat. § 836.05, 2007). According to the U.S. Sentencing Guidelines (U.S.S.G.), "extortion" refers to the "obtaining something of value from another by the wrongful use of (A) force, (B) fear of physical injury, or (C) threat of physical injury." As underlined in U.S. v. Petrovic (2012), "something of value" does include money, property, an advantage, and even sexual relationships.

Extortionate threats intend to induce the belief that victims' power, wealth, security, or reputation are or would be negatively affected. The extortionists use threats in order to

obtain property, not just to dispossess the victims of it (Scheidler v. National Organization for Women, 2003) or services. The "obtaining property from another 'with his consent' induced by wrongful use of threats": consent is "coerced when it is obtained by threat or force" (Green, 2005: 553).

Threats to commit an unlawful act are "extortion" if the threat "is to be carried out in the future" (Berman, 1998: 853). To extort their victims, perpetrators threaten to do a number of things, for instance, to disclose personal data or to post online sexual images or videos (even when these were obtained or recorded illegally), in order to harm the reputation of the victim; to publish libels; to falsely accuse the victim; to rape; to injure property of the person of another; etc.

As explained by Shavell (1993: 1878), offenders should be credible, so that victims would assess that there is "significant chance that the threat will be carried out if and only if he does not accede to it," and, additionally, that, if the offenders are rewarded, the victim "will gain thereby and not merely set himself up for further threats". However, as certain cases demonstrated, victims that give in to extortionate threats are likely to be suffer continued, repeated demands by the perpetrators, situation that can morph into a dominance-subordination relationship. Moreover, extortion is sometimes perpetrated in connect with other offenses, such as money laundering; enticing a minor to engage in illegal sexual activity (U.S. v. Fontana, 2017); credit card fraud (U.S. v. Sunmola, 2018); etc.

Extortionist's motivation can be financial, political, self-gratification, or interpersonal manipulation: "feeling of power and control" (U.S. v. Killen, 2018). Cyber extortion can take numerous forms: justice influence, sexual coercion and extortion (SCE); child sexual exploitation (CSE) (Europol, 2019); etc.

The main forms of sexual coercion and extortion are content driven (for sexual purposes) and financially driven (for economic gain) (Europol, 2016). In certain cases, the demands refer to highly disturbing content, such as rape, bondage, or bestiality images or recordings. According to Europol (2017), about 70% of European countries reported cases of sexual coercion and/or extortion of minors, with over 70% of sexual extortion cases involving only minors.

While children are particularly vulnerable to forms of cyber sexual extortion, the victims of cyber extortion come from a large variety of professional environments. In White v. U.S. (2019), for instance, with the intent to extort the dismissing of state charges against members of a white supremacist group, the defendant threatened to "kidnap, rape, and murder" a judge, the State Attorney, and an agent.

In U.S. v. Coss (2012), on the other hand, a well-known actor partied with two girls, involving the use of illegal drugs, with a number of "bad" photographs taken. The defendants-appellants subsequently created two fictitious personas, used for communications in which they claimed to be a seventeen-year-old girl, impregnated by the recipient of the communication. The defendants-appellants claimed to have compromising photographs, and threatened to sell those photos to a tabloid, unless the victim purchased the photographs.

Often, perpetrators aim to obtain self-generated explicit materials (SGEM), self-generated indecent material (SGIM) (U.S. v. Killen, 2018; Europol, 2019), or child sexually abusive materials (CSAM). In one illustrative case, the perpetrator threatened to "blow up" the computer of a 13-year-old girl, who did believe the the offender could

carry out the threat and engaged in explicit sexual conduct over Skype (Paul, 2015).
Another illustrative case of cyber extortion is U.S. v. Fontana (2017), where the defendant, posing as a minor boy, on a chat website, asked a minor female to take off her shirt. Without victim's knowledge, the defendant recorded the act and threatened the publishing it online, in order to force the victim to "perform more, increasingly invasive sexual acts, which he recorded and used as additional leverage." Similarly, in U.S. v. Petrovic (2012), after the victim informed the defendant that she ends the relationship, the latter threatened to post on the Internet their secretly recorded sexual encounters, so that victim's family could see the videos, if the relationship did end.
In recent years, cyber extortionists, in order to primarily steal photos or videos from victims' devices, or to coerce the victims into providing photos, videos, or live streaming, increasingly employ sophisticated means, such as the use of computer contaminants; cybersquatting; doxing; hacking; and denial of service (DDoS) attacks. There has been a notable increase in the use of ransomware or cryptoware (for instance, WannaCry or Petya/NotPetya), a special form of computer contaminant, which, often through targeted phishing attacks, can rapidly infect numerous victims, allowing criminals to encrypt or withhold data on victims' computer systems and, in exchange for unlocking it, demand payment (ransom), often demanding the ransom to be paid in bitcoins (Europol, 2017; Choi, Scott, & LeClair, 2016).
In an illustrative case, the defendant, in an attempt to hide his identity and to obtain nude photos and videos, used computer contaminants to covertly infiltrate systems and remotely access victim's web cams (U.S. v. Abrahams, 2013). The perpetrator made extortionate threats, to post publicly the photos and videos to victims' social media accounts, unless they received more nude photos and videos.
Cybersquatting, as used for extortion purposes, consists in the registration of Internet domain names involving personal names, followed by attempts to monetize the situation, by offering "reputation management services" to the victims (Randazza v. Cox, 2013). Another notable extortion method is doxing, "the practice of disclosing a person's identifying information (e.g., their home address) on the Internet to retaliate against and harass the 'outed' person" (Vangheluwe v. Got News, 2019: 852), practice that can facilitate or incite to violence against people or groups of people. System hacking or web bots that can launch DDoS attacks (Vasiu & Vasiu, 2014) are also used to create extortion-type situations.

Conclusion

The mass adoption of digital services by consumers and organizations represents a major socio-cultural and economic driver, however, it also brought numerous negative side effects, such as large opportunities for pernicious speech.
Cyber threatening and extortionate communications, especially in their severe forms, can have very serious consequences for victims: cause significant social or economic harm; place the victims in a state of fear or distress; disrupt the normal course of activities; influence how people react or interact. Such communications, therefore, must be addressed promptly and effectively, as means to defend personal safety, fundamental human rights, and sustainable development.

This article provides a comprehensive description of the main characteristics of the phenomenon, including forms, communication vectors, and consequences for victims. Even though the prevalence rates are difficult to assess, this research demonstrates that the scope, effects, and challenges related to the cyber threats and extortion phenomenon are very significant and require a more proactive and dissuasive approach, part of the national cybersecurity strategies.

To control this phenomenon, it is necessary to better understand the initiation, transmission, and escalation of these communications, and to strengthen the legislation as appropriate. There is also a clear need to form threat assessment professionals, to develop best practice guidelines for law enforcement agents, to facilitate information sharing and coordinated actions among stakeholders, and to provide effective civil code solutions.

Linguistic research on these communications and the development of effective deep read textual analysis tools should receive more consideration. Such tools would allow the prediction or identification of threatening and extortionate communications and could improve significantly the prevention activity. Advanced software solutions can also play an important role in the filtering out of such communications, trigger accounts termination, and refer such instances to appropriate law enforcement agencies, for timely reactions.

The expenditure for programs that address related aspects, such as hate speech, gender inequality, and forms of group-based harassment, should be be increased. Awareness and education can also play an important role in controlling this phenomenon, and must include aspects regarding the cyber risks, protection of personal data and privacy, preservation of digital evidence, adequate reactions to these threats, and law enforcement incident reporting.

References

Berman, M.N. (1998). The Evidentiary Theory of Blackmail: Taking Motives Seriously. *University of Chicago Law Review*, *65*, 795-878.

Choi, K., Scott, T.M., & LeClair, D.P. (2016). Ransomware against Police: Diagnosis of Risk Factors via Application of Cyber-Routine Activities Theory. *International Journal of Forensic Science & Pathology*, *4*, 253-258.

Commonwealth v. Knox, 190 A.3d 1146 (Pa. 2018).

Cybercrime Convention Committee. (2018). Mapping Study on Cyberviolence.

European Institute for Gender Equality. (2017). Cyber violence against women and girls.

Europol. (2016). Internet Organised Crime Threat Assessment.

Europol. (2017). Internet Organised Crime Threat Assessment.

Europol. (2019). Internet Organised Crime Threat Assessment.

Eisenberg, A.K. (2015). Criminal Infliction of Emotional Distress. *Michigan Law Review, 113*, 607-662.

Green, S.P. (2005). Theft by Coercion: Extortion, Blackmail, and Hard Bargaining. *Washburn Law Journal*, *44*, 553-582.

Han, D.S. (2014). The Mechanics of First Amendment Audience Analysis. *William and Mary Law Review*, *55*, 1647-1717.

Harawa, D.S. (2014). Social Media Thoughtcrimes. *Pace Law Review*, *35*, 366-397.

Leary, M.R., Twenge, J.M., & Quinlivan, E. (2006). "Interpersonal Rejection as a Determinant of Anger and Aggression. *Personality and Social Psychology Review*, *10*, 111-132.

Paul, J. (2015). Ohio Man Sentenced in Jefferson County for Sexually Exploiting Teen. *Denver Post*. Retrieved from http://www.denverpost.com/news/ci_27306114/ohio-man-sentenced-jefferson-county-sexually-exploiting-teen.

Peters, G. J. Y., Ruiter, R. A., & Kok, G. (2014). Threatening communication: A qualitative study of fear appeal effectiveness beliefs among intervention developers, policymakers, politicians, scientists, and advertising professionals. *International Journal of Psychology*, *49(2)*, 71-79.
Peterson, J. & Densley, J. (2017). Cyber Violence: What Do We Know and Where Do We Go From Here? *Aggression and Violent Behavior*, *34*, 193-200.
RAV v. St. Paul, 505 U.S. 377 (1992).
Randazza v. Cox, 920 F. Supp. 2d 1151 (D. Nev. 2013)
Romney, J. (2012). Eliminating the Subjective Intent Requirement for True Threats in United States v. Bagdasarian. *Brigham Young University Law Review, 2012*, 639-654.
Scheidler v. National Organization for Women, 537 U.S. 393 (2003).
Shavell, S. (1993). An Economic Analysis of Threats and Their Illegality: Blackmail, Extortion, and Robery. *University of Pennsylvania Law Review*, *141*, 1877-1903.
Spitzberg, B.H., & Gawron, J.M. (2016). Toward Online Linguistic Surveillance of Threatening Messages. *Journal of Digital Forensics, Security and Law*, *11*, 43-77.
United Nations. (2015). Sustainable Development Goals. Retrieved from http://www.un.org/sustainabledevelopment/
U.S. v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997).
U.S. v. Bagdasarian, 652 F.3d 1113 (9th Cir. 2011).
U.S. v. Bishop, Case 118MJ24LDA (D.R.I. January 23, 2018).
U.S. v. Cain, No. 1: 16-cr-00103-JAW (D. Me. June 1, 2018).
U.S. v. Coss, 677 F.3d 278 (6th Cir. 2012).
U.S. v. Davis, No. 18-4201 (4th Cir. Jan. 21, 2020).
U.S. v. Fontana, No. 16-2208 (6th Cir. Aug. 25, 2017).
U.S. v. Haileselassie, No. 18-1343 (8th Cir. June 10, 2019).
U.S. v. Heineman, 767 F.3d 970, 972 (10th Cir. 2014).
U.S. v. Humphries, No. 12 Cr. 347 (RWS) (S.D.N.Y. Oct. 28, 2013).
U.S. v. Jordan, No. 16-CR-93-FPG-HKS-1 (W.D.N.Y. Oct. 24, 2017).
U.S. v. Killen, No. 15-15001 (11th Cir. Mar. 29, 2018).
U.S. v. Leach, Criminal Complaint, Case No. 2:17mj-44-1 (D. Vt. Apr. 21, 2017).
U.S. v. Michael, No. 2: 12-cr-1-WTL-CMM (S.D. Ind. Oct. 9, 2012).
U.S. v. Parr, 545 F.3d 491 (7th Cir. 2008).
U.S. v. Petrovic, 701 F.3d 849 (8th Cir. 2012).
U.S. v. Sunmola, 887 F.3d 830 (7th Cir. 2018).
U.S. v. Swarbrick, Case 3:18-MJ-1214 (M.D. Tenn. Sep. 19, 2018).
U.S. v. Turrella, No. 10-30051 (9th Cir. 2012).
U.S. v. Twine, 853 F.2d 676, 678 (9th Cir. 1988).
U.S. v. Twitty, Criminal Case No. 13-CR-00076-RBJ (D. Colo. Jan. 4, 2019).
U.S. v. Vandevere, No. 1: 19-cr-63-MOC (W.D.N.C. Sept. 16, 2019).
U.S. v. Wheeler, Criminal Case No. 12-cr-0138-WJM (D. Colo. July 9, 2019).
U.S. v. Whitmore, No. 17-11753, Non-Argument Calendar (11th Cir. Sept. 19, 2019).
U.S. v. Williams, No. 17-2454 (8th Cir. Oct. 26, 2018).
van der Wilk, A. (2018). Cyber violence and hate speech online against women. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs.
Vangheluwe v. Got News, LLC, 365 F. Supp. 3d 850 (E.D. Mich. 2019).
Vasiu, I., & Vasiu, L. (2014). Break on Through: An Analysis of Computer Damage Cases. *Pittsburgh Journal of Technology Law & Policy*, *14*, 158-201.
Volokh, E. (2016). The Freedom of Speech and Bad Purposes. *UCLA Law Review*, *63*, 1366-1421.
Warren, L.J., Ogloff, J.R.P., & Mullen, P.E. (2013). The Psychological Basis of Threatening Behaviour. *Psychiatry, Psychology and Law, 20*, 329-343.
White v. U.S., No. 6: 17-cv-689-Orl-28GJK (M.D. Fla. Feb. 14, 2019).
Women and Gender Equality Canada. (2019). New federal investment will help end cyberviolence. Retrieved from https://www.canada.ca/en/status-women/news/2019/08/new-federal-investment-will-help-end-cyberviolence.html.