DOI 10.5817/MUJLT2020-1-1

CYBER EXTORTION AND THREATS: ANALYSIS OF THE UNITED STATES CASE LAW

by

IOANA VASIU[*], LUCIAN VASIU[**]

This article presents an analysis of the cyber extortion and threats cases brought to the United States courts. The inquiry employed content analysis to identify important elements and attributes and answers research questions concerning essential attributes, legal elements, and how do the courts interprets these offenses. The article extends the understanding of this phenomenon by providing a thorough discussion of the conceptual issues and characteristics and an analysis of the most important litigation aspects, such as intent, true threats, sentencing, and the insanity defense. The article concludes with recommendations for stakeholders, to more effectively address the phenomenon.

KEY WORDS

Cybercrime, Extortion, Insanity, Intent, Malware, Sentencing, Speech, True Threats

[*] ioanav3@yahoo.com, Prof. Dr., Faculty of Law; Coordinator of the *BBU Faculty of Law's Cybercrime Research Unit*; member of the *BBU Scientific Council*; member of the *Board of Directors* of the *International Association of Penal Law* (2014–2024); and external affiliated member of the *Ostrom Workshop Program on Cybersecurity and Internet Governance, Indiana University*. Expert with the *European Commission* and the *UNDP Romania*; partner and lead researcher on several projects funded by the *European Commission, Dutch Council for the Judiciary* and other entities; co-Chair of the *Management and Delivery of Justice Group* of the *European Group of Public Administration*; and keynote speaker or moderator at numerous professional events organized by prestigious organizations, such as *OECD* or *UNDP/RCPAR*. Her research focuses on cybercrime nature, prevention, and litigation.

[**] lvcianvs@yahoo.com, PhD, MBA, computer scientist, expert in cybercrime prevention and information systems security.

1. INTRODUCTION

"Cyberviolence" involves 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."*[1]

"Cyberviolence" comprises numerous offenses, among these cyber extortion and threats represent important categories.

Cyber extortion and threats are acts of

> *"conditional speech intended to influence or gain compliance from a target recipient."*[2]

These communications can be effective in gaining the *"feeling of power and control"*[3] over victims.[4] These offenses cover a range of forms, including intimate partner violence (IPV), violence against women and girls (VAWG), cyber dating abuse (CDA) and so on.

It is difficult to quantify the full extent of the phenomenon; however, as it produces significant negative personal, economic, and societal consequences, is regarded as one that needs to be more effectively addressed.[5] This article aims to present an analysis of the phenomenon's

---

[1] Cybercrime Convention Committee (T-CY). (2018) *Mapping Study on Cyberviolence*. [online] Strasbourg: Council of Europe, 5, Available from: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914 [Accessed 1 July 2019].

[2] Spitzberg, B.H. and Gawron, J.M. (2016) Toward Online Linguistic Surveillance of Threatening Messages. *Journal of Digital Forensics, Security and Law*, 11, p. 47.

[3] *United States v. Killen.* (2018) No. 15-15001 (11th Cir.), 29 March.

[4] *Fontana v. United States*. (2020) No. 14-20141 (E.D. Mich.), 17 April; Bumb, M. L. (2017) Domestic Violence Law, Abusers' Intent, and Social Media: How Transaction-Bound Statutes Are the True Threats to Prosecuting Perpetrators of Gender-Based Violence. *Brooklyn Law Review*, 82 (2), pp. 917–960.

[5] See, e.g. Van Der Wilk, A. (2018) *Cyber violence and hate speech online against women*. PE 604.979. Brussels: European Parliament. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf [Accessed 1 July 2019]; U.S. Department of Justice. (2016) *The National Strategy for Child Exploitation Prevention and Interdiction*. [online] Washington: U.S. Department of Justice. Available from: https://www.justice.gov/psc/file/842411/download [Accessed 20 October 2019]; Women and Gender Equality Canada. (2019) *New federal investment will help end cyberviolence.* [press release] 27 August. Available from: https://www.canada.ca/en/status-women/news/2019/08/new-federal-investment-will-help-end-cyberviolence.html [Accessed 3 December 2019]; European Institute for Gender Equality. (2017) *Cyber violence against women and girls*. Available from: https://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls.pdf [Accessed 3 December 2019]; Peterson, J. and Densley, J. (2017) Cyber Violence: What Do We Know and Where Do We Go From Here?. *Aggression and Violent Behavior*, 34, pp. 195–196; Cybercrime Convention Committee (T-CY). (2018) *Mapping*

attributes and of the most important litigation aspects. The analysis is based on a large corpus of data, consisting of several hundred cases brought to the U.S. courts. This inquiry employed content analysis to identify and group important elements and issues. The article answers the following research questions: What are the attributes of the phenomenon? What are the elements of cyber extortion and threats that the legal system addresses? How do the courts interprets these crimes?

The article proceeds in three Sections. The next Section discusses the attributes of the cyber extortion and threats phenomenon. Section 3 outlines the legal framework for these offenses. Section 4, based on the comprehensive study of cases brought to federal courts in violation of the federal threat statute, 18 U.S.C. § 875 (c) & (d), presents an analysis of important litigation aspects: intent, "true threats", sentencing aspects, and the insanity defense. The article concludes with recommendations for stakeholders, to more effectively address the phenomenon.

2. ATTRIBUTES OF THE PHENOMENON

2.1. THREATS

A "threat" is

> *"an avowed present determination or intent to injure presently or in the future."*[6]

There are two main forms of threats: interpersonal and impersonal. Interpersonal threats, which can be encountered in cases of direct relations, in a variety of contexts, are transmitted with a view to obtain recipient's compliance. Impersonal threats target groups of people (for instance, members of law enforcement agencies, civil liberties organizations, minority groups, etc.)[7] or leaders, and can be encountered in cases of perceived

Study on Cyberviolence. T-CY(2017)10. Strasbourg: Council of Europe, 4, Available from: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914 [Accessed 1 July 2019]; European Union Agency for Law Enforcement Cooperation (Europol). (2017) *Internet Organised Crime Threat Assessment*. The Hague: Europol. Available from: https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf [Accessed 1 June 2018].

[6] *United States v. Alkhabaz.* (1997) 104 F.3d 1492 (6th Cir.), 29 January.

[7] See, e.g. *United States v. Jordan.* (2017) No. 16-CR-93-FPG-HKS-1 (W.D.N.Y.), 24 October (the defendant posted on *Facebook* the message *"Lets Start Killin Police Lets See How Dey Like It."*); *United States v. Carrillo.* (2020) No. 1: 19-cr-01991 KWR (D.N.M.), 8 April (the defendant, via *Facebook*, communicated a threat to injure ACLU personnel); *United States v. Doggart.* (2020) 947 F.3d 879 (6th Cir.), 15 January (the defendant planned to destroy a religious community in New York state).

distress or coercion, created by certain pressures (e.g. political, economic, or social).

Threats can be also be categorized as reactive, when responding to real or perceived events or threats (for example, as retaliation[8] or reaction for the loss of social status), and proactive, when attempting to achieve certain goals (to "align" the threateners' desires or wishes and the actual reality).[9] A subcategory of the latter is the infliction of fear for threateners' own gratification or enjoyment.[10]

Threats usually aim to determine the recipient to comply with certain requests, rather than actually engaging with them in the course of action described. Nevertheless, these threats have a complex relationship to actual harm. Such communications can inflict

> *"psychological harm on the listener in the direct manner that a physical attack would inflict physical harm."*[11]

Further, 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."*[12]

Cyber extortion and threats are not new offenses. However, cyberspace and social media platforms, in particular, make much more difficult to determine threateners' actual state of mind and what are the actual capabilities of the threateners with respect to carry out the threats. Additionally, technology permits the transmission of threats using a false identity or the identity of another person,[13] and to reach a large number

---

[8] *United States v. Telfair.* (2020) No. 19-CR-270 (E.D.N.Y.), 3 February (the defendant threatened a witness who testified against the defendant's brother in a criminal case).

[9] See Criminal Complaint, *United States v. Swarbrick.* (2018) Case 3:18-MJ-1214 (M.D. Tenn.), 19 September. Available from: https://www.courthousenews.com/wp-content/uploads/2018/09/EricSwarbrick.pdf (in an attempt to meet with a famous singer, the defendant sent tens of threatening letters and e-mails) [Accessed 1 June 2019].

[10] See, e.g. *United States v. Haileselassie.* (2019) No. 18-1343 (8th Cir.), 10 June (the defendant made bomb threats at a community college).

[11] Han, D.S. (2014) The Mechanics of First Amendment Audience Analysis. *William and Mary Law Review*, 55, pp. 1647, 1659.

[12] Romney, J. (2012) Eliminating the Subjective Intent Requirement for True Threats in United States v. Bagdasarian. *Brigham Young University Law Review*, 2012, pp. 639, 653.

[13] See *United States v. Turrella.* (2012) No. 10-30051 (9th Cir.), 15 March.

of people, potentially amplifying the fear or the anxiety.[14] Even more disturbing, threats can be of the anti-social type, transmitted anonymously,[15] and could reach people (online viewers or followers), who, in turn, may potentially be encouraged or willing to fulfill the call for violent actions, thus producing a spread or proliferation effect.

The communication of threats can be brought about by numerous motivational states, rational or irrational. The threatening content can regard personal honor or dignity, incitement to discrimination, or violent actions against certain people or groups of people. To achieve their objective, threateners use a range of threats: to injure the property, reputation, or the person of another, to kidnap or kill the victims.

The language employed in the communications can be clear, but also implied, veiled, or cryptical.[16] In a number of cases, the language used is truly malignant, sadistic and extreme. To illustrate the point through a few examples, the defendant in *United States v. Wheeler* threatened to

> *"kill cops[,] drown them in the blood of thier [sic] children, hunt them down and kill their entire bloodlines;"*[17]

in *United States v. Cain*, the defendant, in brutal terms, threatened to kill his ex-wife, her mother and her new boyfriend, to send to members of ex-wife's family videotapes showing the victim engaged in sexual acts, and to rape victim's daughter;[18] in *United States v. Heineman*, the defendant, a white supremacy sympathizer, sent to the victim e-mails containing 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!;"*[19]

in *United States v. Williams*, the defendant threatened to kill a judge,

---

[14] See Criminal Complaint at 2 et seq., *United States v. Bishop.* (2018) Case 118MJ24LDA (D.R.I.), 23 January (defendant sent hundreds of threatening e-mails to his former girlfriend, her family, and three state prosecutors, victims expressing "extreme fear for their safety").

[15] See, e.g. *United States v. Bagdasarian.* (2011) 652 F.3d 1113 (9th Cir.), 19 July (on a *Yahoo* message board, the defendant posted threats anonymously).

[16] See, e.g. Memorandum Opinion and Order at 18, *United States v. White.* (2010) Criminal Action No. 7:08-CR-00054 (W.D. Va.), 20 January.

[17] See, e.g. *United States v. Wheeler.* (2019) Criminal Case No. 12-cr-0138-WJM (D. Colo.), 9 July.

[18] *United States v. Cain.* (2018) No. 1: 16-cr-00103-JAW (D. Me.), 1 June.

[19] *United States v. Heineman.* (2014) 767 F.3d 970, 972 (10th Cir.), 15 September.

> *"sodomize the corpse, chop it into pieces, and mail one piece of the corpse to the courthouse each week."*[20]

The inclusion of unsettling images, as means to make the "message" more powerful, can also be noted: in *United States v. Vandevere*, for instance, the defendant sent a "tweet" that contained a lynching picture.[21]

There are numerous threat communication means, mainly e-mail;[22] telephone;[23] online call spoofing services;[24] and social media platforms. In *United States v. Michael*, to illustrate the latter, the defendant posted on *Facebook* threats to *"kidnap and injure DEA agents and personnel"* and that it's

> *"time we answered their crimes with bloodshed and torture."*[25]

In *Commonwealth v. Knox*, for another example, the appellant recorded and uploaded to *YouTube* a rap song titled *"F--k the Police"*.[26] The song's lyrics expressed hatred and contained

> *"descriptions of killing police informants and police officers."*[27]

The court held that the

> *"threats to the officers were real, specific and violent, with nothing of record to indicate that the threats should not be taken seriously"*

---

[20] *United States v. Williams.* (2018) No. 17-2454 (8th Cir.), 26 October.

[21] *United States v. Vandevere.* (2019) No. 1: 19-cr-63-MOC (W.D.N.C.), 16 September.

[22] See, e.g. *United States v. White.* (2017) Criminal Action No. 7: 13CR00013 (W.D. Va.), 31 May (the defendant sent several e-mails, threatening to injure his ex-wife, if she did not send him "alimony" payments); *United States v. Gillenwater.* (2014) 749 F.3d 1094 (9th Cir.), 11 April (defendant sent an e-mail threatening the life of another); *United States v. McCrudden.* (2015) No. CR-11-061 (DRH) (E.D.N.Y.), 16 March (defendant sent an e-mail claiming that he hired people to kill the victim).

[23] See, e.g. Criminal Complaint, *United States v. Lisnyak.* (2015) Case No. 15-04179MJ-PCT-DMF (D. Ariz.), 16 July; *United States v. Champ, United States v. Wood.* (2006) 459 F. Supp. 2d 451 (E.D. Va.), 29 September.

[24] See, e.g. Criminal Complaint, *United States v. Kadar.* (2017) Case No. 6:17-mj-1361 (M.D. Fla.), 4 April at 4.

[25] *United States v. Michael.* (2012) No. 2: 12-cr-1-WTL-CMM (S.D. Ind.), 9 October.

[26] *Commonwealth v. Knox.* (2018) 190 A.3d 1146, 1149 (Pa.), 21 August.

[27] Op. cit., at 1149.

or that the defendants would not be able to *"carry them out."*[28] The fervency of threats can be increased through repeat communications and the use of multiple means.[29]

2.2. EXTORTIONATE THREATS

"Extortion" encompasses numerous forms and has multiple definitions. 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."*[30]

According to the *U.S. Sentencing Guidelines (U.S.S.G.)*, "extortion" refers to

> *"obtaining something of value from another by the wrongful use of (A) force, (B) fear of physical injury, or (C) threat of physical injury."*

"Something of value" includes money, property, an advantage, or even a sexual relationship.[31]

Extortionate threats cover the making or implying of threats that intend to induce the belief that victim's power, wealth, social standing, personal or job security, or self-esteem are or could be endangered. The extortionist must use threats with a view to "obtain" or "acquire" property, not just to deprive or dispossess the victim of it.[32] An important element of extortion is

> *"that of obtaining property from another 'with his consent' induced by wrongful use of threats."*[33]

Professor Steven Shavell, the Director of the *John M. Olin Center for Law, Economics, and Business* at the *Harvard Law School*, explains that threateners

---

[28] Op. cit., at 1174.

[29] See Criminal Complaint, *United States v. Leach.* (2017) Case No. 2:17mj-44-1 (D. Vt.), 21 April (the defendant transmitted repeated death threats, via *Facebook*, e-mail, and telephone).

[30] 2019 Florida Statutes 836.05 Threats; extortion. In English. Available from: http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=0800-0899/0836/Sections/0836.05.html [Accessed 1 July 2019].

[31] *United States v. Petrovic.* (2012) 701 F.3d 849 (8th Cir.), 13 December.

[32] *Scheidler v. National Organization for Women.* (2003) 537 U.S. 393, 26 February.

[33] Green, S.P. (2005) Theft by Coercion: Extortion, Blackmail, and Hard Bargaining. *Washburn Law Journal,* 44, p. 553 (the consent is *"coerced when it is obtained by threat or force"*).

must make credible threats, so that the victims would believe that there is

> *"significant chance that the threat will be carried out if and only if he does not accede to it,"*

and, if the threateners are rewarded, the victim

> *"will gain thereby and not merely set himself up for further threats."*[34]

Nevertheless, as seen in a number of cases, the victims that gave in to extortionate threats are likely to be suffer continued, repeated demands from the perpetrators, a situation that can become a prolonged or extended dominance-subordination relationship.

Threats to commit an unlawful act amount to "extortion" if the threat *"is to be carried out in the future."*[35] To extort their victims, perpetrators may threaten to, for instance, damage the victim's property or reputation (for example, by releasing damaging photos and videos[36] or libelous material), or even falsely accuse the victim.[37] Some of the main forms of extortion include the influence of justice, sextortion,[38] sexual coercion and extortion (SCE), reputation damage,[39] etc. In *White v. United States*, for illustration, the defendant, with the intent to extort the dismissing of the state charges against members of a white supremacist group, threatened to *"kidnap, rape, and murder"* a judge, the State Attorney, and a federal agent, to behead them, and to paint on walls with their blood.[40]

In a number of cases, as the result of the extortion of victims, perpetrators aimed to obtain self-generated explicit materials (SGEM) or self-generated indecent material (SGIM).[41] In *United States v. Fontana*, for example, the defendant, posing as a minor boy on a chat website, asked

---

[34] Shavell, S. (1993) An Economic Analysis of Threats and Their Illegality: Blackmail, Extortion, and Robbery. *University of Pennsylvania Law Review*, 141, p. 1878.

[35] Berman, M.N. (1998) The Evidentiary Theory of Blackmail: Taking Motives Seriously. *University of Chicago Law Review*, 65, pp. 795, 853.

[36] See *United States v. Gomez.* (2020) No. 18-12089 (11th Cir.), 14 February.

[37] *United States v. Avenatti.* (2020) No.(S1) 19 Cr. 373 (PGG) (S.D.N.Y.), 14 January.

[38] This form of extortion is characterized by threats that aim to humiliate the victim by posting online compromising sexual images or recordings. For instance, the distribution of videos, unless the suspects receive monetary compensation, see, e.g. *In the Matter of Search of a Residence in Oakland.* (2019) Case No. 4-19-70053 (N.D. Cal.), 10 January.

[39] See *United States v. Coss.* (2012) 677 F.3d 278 (6th Cir.), 16 April: threatening to injure someone's reputation, the threat must be "wrongful" but it need not be independently illegal.

[40] *White v. United States.* (2019) No. 6: 17-cv-689-Orl-28GJK (M.D. Fla.), 14 February.

[41] *United States v. Killen.* (2018) No. 15-15001 (11th Cir.), 29 March.

a minor female to take off her shirt.[42] Without the victim's knowledge, the defendant recorded the act and subsequently threatened to publish online of the recording, in order to "take over" the victim's life and force her to

> *"perform more, increasingly invasive sexual acts, which he recorded and used as additional leverage."*[43]

In *United States v. Abrahams*[44], the defendant, to hide his identity and to obtain nude photos and videos, used malware and other computer tools, to operate remotely the victims' web cams, without their consent. The perpetrator made extortionate threats of publicly posting the compromising photos or videos to the victims' social media accounts, unless the latter sent more nude photos or videos.[45]

3. LEGAL FRAMEWORK

Depending on the circumstances surrounding each case, several federal threat statutes can be applicable, such as 18 U.S.C. § 115 (influencing, impeding, or retaliating against a Federal official by threatening or injuring a family member);[46] 18 U.S.C. § 248 (freedom of access to clinic entrances);[47] 18 U.S.C. § 871 (threats against the President and successors to the Presidency);[48] 18 U.S.C. § 1512 (tampering with a witness, victim, or an informant);[49] 18 U.S.C. § 2332a (use of weapons of mass destruction).[50]

---

42 *United States v. Fontana.* (2017) No. 16-2208 (6th Cir.), 15 August.

43 Ibid.

44 Complaint. *United States v. Abrahams.* (2013) No. 8:13-mj-00422 (C.D. Cal.), 17 September. See also *United States v. Chansler.* (2010) No. 3:10-cr-00100 (M. D. Fla.), 15 April. (the defendant enticed the victim to send him sexually explicit images and videos, then threatened to injure the victim's reputation through the release of the materials online or to the victims' friends or family, unless he received more such materials).

45 Ibid.

46 See *United States v. Cruz.* (2017) No. 15-3139 (3d Cir.), 8 November (threatening to assault and kill a United States Department of Homeland Security agent).

47 See *United States v. Dillard.* (2011) 835 F. Supp. 2d 1120 (D. Kan.), 21 December.

48 See *United States v. Dutcher.* (2017) 851 F.3d 757 (7th Cir.), 22 March (the defendant announced on *Facebook* his plan to assassinate President *Obama*); *United States v. Christy.* (2019) No. 3: 18-CR-223 (M.D. Pa.), 14 February (the defendant posted on *Facebook* that he was *"going to shoot President Donald J. Trump in the head"*).

49 See, e.g. *United States v. Springer.* (2018) No. 17-15584, Non-Argument Calendar (11th Cir.), 26 October [the defendant, sympathizer of a terrorist organization, threatened to assault and murder a judge, in violation of 18 U.S.C. § 115(a)(1)(B); attempted to obstruct justice, in violation of 18 U.S.C. §§ 1503 and 2; and attempted to tamper with witnesses, in violation of 18 U.S.C. §§ 1512(b)].

50 *United States v. Parr.* (2008) 545 F.3d 491 (7th Cir.), 18 September (the defendant threatened to use a weapon of mass destruction against a federal government building).

Most cases of electronic threats are brought to courts in violation of 18 U.S.C. § 875(c):

> *"Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both."*

Extortionate threats, on the other hand, following the manner in which they are committed, can be prosecuted in violation of a number of sections, such as 18 U.S.C. § 875(b) (interstate communications with intent to extort);[51] 18 U.S.C. § 1030(a)(7) (transmitting, with intent to extort, communication containing threat to cause damage);[52] 18 U.S.C. § 1951 (interfering with commerce by robbery, extortion, threats or violence); 18 U.S.C. § 844(e) (making interstate threats related to explosives).[53] Most often, however, cyber extortion cases are brought to courts in violation in violation of 18 U.S.C. § 875(d):

> *"Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both."*

4. LITIGATION ASPECTS

Cyber-extortion and threats can be encountered in many forms and contexts, thus allowing interpretations at numerous levels, as well as interesting arguments and viewpoints to emerge. The following subsections illustrate aspects concerning intent, "true threats", sentencing, and the insanity defense.

---

[51] See *United States v. Smith.* (2017) 878 F.3d 498 (5th Cir.), 28 December; *United States v. Williams.* (2012) 693 F.3d 1067 (9th Cir.), 7 September.

[52] See, e.g. *United States v. Fowler.* (2010) Case No. 8:10-cr-65-T-24 AEP (M.D. Fla.), 25 October (upon being fired, the defendant accessed victim's computers and changed employees' and the firewall passwords); *United States v. Ivanov*. (2001) 175 F. Supp. 2d 367 (D. Conn.), 6 December (the defendant gained unauthorized control over victim's computer network, then threatened the victim with the destruction of its computer systems).

[53] See Criminal Complaint, *United States v. Kadar.* (2017) 6:17-mj-1361 (Fla.), 4 April.

4.1. INTENT

Criminal liability arises only when if a person, during the perpetration of the offense, had a guilty state of mind.[54] The *U.S. Model Penal Code* lists four levels of intent: purpose,[55] knowledge,[56] recklessness,[57] and negligence[58] (from greatest to least culpability).

"Intent" has numerous meanings,[59] the judicial outcome depending upon the meaning embraced by the court.[60] As underlined in *United States v. Heineman*[61], background norms for construing criminal statutes, which

> *"presume that intent [i.e. something more than negligence] is the required mens rea in criminal laws."*

Clearly, without the unambiguous determination of a defendant's criminal intent, there can be unintended consequences.

The determination of "intent" offers interesting arguments and examinations. In *United States v. Wheeler*, for example, the court held that

> *"it is not necessary to show that a defendant intended to or had the ability to actually carry out the threat."*[62]

However, in *United States v. Gossett*[63], the defendant argued that evidence that he intended or had the ability to carry out the threats is relevant, as it *"may bear on the requisite mens rea,"* and the court agreed.

---

[54] See Collins, E. (2018) Insane: James Holmes, Clark v. Arizona, and America's Insanity Defense. *Journal of Law and Health*, 31, p. 33; Kachulis, L. (2017) Insane in the Mens Rea: Why Insanity Defense Reform is Long Overdue. *Southern California Interdisciplinary Law Journal*, 26, pp. 357, 362.

[55] *U.S. Model Penal Code*, General Requirements of Culpability, § 2.02(2)(a)(i). Philadelphia: American Law Institute. In English.

[56] *U.S. Model Penal Code*, General Requirements of Culpability, § 2.02(2)(b)(ii). Philadelphia: American Law Institute. In English.

[57] *U.S. Model Penal Code*, General Requirements of Culpability, § 2.02(2)(c). Philadelphia: American Law Institute. In English.

[58] *U.S. Model Penal Code*, General Requirements of Culpability, § 2.02(2)(d). Philadelphia: American Law Institute. In English.

[59] See, e.g. Crump, D. (2010) What Does Intent Mean? *Hofstra Law Review*, 38, p. 1059 (arguing that the appropriate definition of "intent" *"should depend upon factors such as the likely availability of proof, the seriousness of the offense or tort, its severity within a hierarchy of other offenses, and the difficulty of otherwise distinguishing innocent conduct"*).

[60] Op. cit., p. 1061.

[61] *United Stated v. Heineman.* (2014) 767 F.3d 970, 986-7 (10th Cir.), 14 September (citing *Judge Sutton's* dubitante opinion).

[62] *United States v. Wheeler.* (2015) 776 F.3d 736, 743 (10th Cir.), 15 January.

[63] *United States v. Gossett.* (2019) No. 1: 19-cr-00081 WJ (D.N.M.), 7 May.

An important decision can be found in *Elonis v. United States*[64], a case that received very significant attention from the legal commentators.[65] Elonis raised important questions regarding convictions under 18 U.S.C. § 875(c): whether proof of the defendant's subjective intent to threaten and proof of a defendant's subjective intent to threaten are required. The *Supreme Court* held that, even though there is no required mental state specified in the statute, it *"does not mean that none exists"*.[66] Further, the *Supreme Court* underlined that convictions under Section 875(c) cannot be based solely on a reasonable person's interpretation of the defendant's communication, however, it did not specify what *mens rea* is required under this section, reasoning only that the simple negligence standard should be construed unconstitutional.[67] Since "intent" may not be proven directly, in order to make a determination, the courts often examine the circumstances and the context associated with the defendants' actions.

Unlike Section 875(c), Section 875(d) does contain a required mental state: the intent to extort, consequently *Elonis* does not apply to prosecutions under Section 875(d). Extortion generally refers to the intent to obtain money or other thing of value with a person's consent induced by the wrongful use of actual or threatened fear, violence, or force.[68]

In order to prove the intent to extort, prosecutors must demonstrate that the defendant, through wrongful conduct, did have the intent to procure something of value,[69] without the need to demonstrate that the defendant actually intended to carry out the threats communicated. As the court in *United Stated v. Killen* held,

---

[64] *Elonis v. United States.* (2015) 135 S. Ct. 2001, 575 U.S., 192 L. Ed. 2D 1, 1 June.

[65] See, e.g. Quek, J.X. (2016) Elonis v. United States: The Next Twelve Years. *Berkeley Technology Law Journal*, 31, p. 1109; Brusco, M.A. (2016) Read This Note or Else!: Conviction Under 18 U.S.C. § 875(c) for Recklessly Making a Threat. *Fordham Law Review*, 84, p. 2845; Barney, D. (2016) Elonis v. United States: Why the Supreme Court Punted on Free Speech. *Pepperdine Law Review*, 2016, p. 1; Roark, M.M. (2015) Elonis v. United States: The Doctrine of True Threats: Protecting Our Ever-Shrinking First Amendment Rights in the New Era of Communication. *Pittsburgh Journal of Technology Law & Policy*, 15, p. 197; Pierce, M. (2015) Prosecuting Online Threats After Elonis. *Northwestern University Law Review*, 110, p. 51; Geha, G. (2016) Think Twice Before Posting Online: Criminalizing Threats Under 18 U.S.C. § 875(c) After Elonis. *John Marshall Law Review*, 50, p. 167.

[66] *Elonis v. United States.* (2015) 135 S. Ct. 2001, 575 U.S., 192 L. Ed. 2d 1 at 2009, 1 June.

[67] Op. cit., at 2012–13.

[68] U.S. Department of Justice. (2010) *Prosecuting Computer Crimes*. [online] Washington: Office of Legal Education Executive Office for United States Attorneys, p. 53. Available from: https://justice.gov/criminal/cybercrime/docs/ccmanual.pdf [Accessed 30 October 2012].

[69] See *United Stated v. Killen.* (2018) No. 15-15001, 11th Cir., 29 March.

"[e]xtortion only works if the [victim] fears that not paying will invite an unsavory result,"

"to intend to extort one must necessarily intend to instill fear of harm."[70]

The court further argued that

"it would be passing strange, indeed impossible, for a defendant to intend to obtain something by communicating [...] a threat [to injure the property or reputation of another or a threat to accuse another of a crime] without also intending, understanding, or, possibly, recklessly disregarding that the communication would be perceived as threatening."[71]

4.2. TRUE THREATS

The First Amendment stipulates that

"Congress shall make no law [...] abridging the freedom of speech."[72]

There are, however, categories of speech which do not fall under this protection, such as

"advocacy intended and likely to incite imminent lawless action, obscenity, defamation, child pornography, fighting words, fraud, true threats, speech integral to criminal conduct, and speech presenting a grave and imminent threat the government has the power to prevent."[73]

These aspects were analyzed extensively by numerous legal commentators.[74] The prosecution, nonetheless,

"is not permitted to punish speech merely because the speech is forceful or aggressive."[75]

For instance, if a person suggests "revenge", this does not necessarily imply breach of any law.[76] To further complicate things, many harms that could be

[70] Ibid.

[71] Ibid.

[72] *The Constitution of the United States 1788 (Amendment I)*. United States of America. In English.

[73] Harawa, D.S. (2014) Social Media Thoughtcrimes. *Pace Law Review*, 35, pp. 366, 380.

[74] See, e.g. Volokh, E. (2016) The Freedom of Speech and Bad Purposes. *UCLA Law Review*, 63, p. 1366; Coenen, D.T. (2017) Freedom of Speech and the Criminal Law. *Boston University Law Review*, 97, p. 1533.

[75] *United States v. Schweitzer.* (2017) No. 4: 17CR3094 (D. Neb.), 28 November.

[76] See Strasser, M. (2011) Advocacy, True Threats, and the First Amendment. *Hastings Constitutional Law Quarterly*, 38, p. 339.

caused by threats, might also be caused by advocacy, for instance, certain political messages are *"threatening and should nonetheless be protected".*[77]

The true threats prohibition *"protect[s] individuals from the fear of violence"* and *"from the disruption that fear engenders,"* and protects people

> *"from the possibility that the threatened violence will occur".*[78]

A communication can be considered "threat" if

> *"it expresses an intention to inflict harm, loss, evil, injury, or damage on another."*[79]

Nevertheless, numerous factors are taken into consideration in the determination of "true threats," for instance,

> *"the reaction of the recipient of the threat and of other listeners; whether the threat was conditional; whether the threat was communicated directly to its victim; whether the maker of the threat had made similar statements to the victim in the past; and whether the victim had reason to believe that the maker of the threat had a propensity to engage in violence."*[80]

A defendant's background can often be considered relevant towards the determination of a "true threat".[81]

The courts disagree on how "true threat" should be defined.[82] The majority of courts use the "objective test", which examines whether a reasonable person would regard the threat as true. Nevertheless, based on the *Supreme Court's* decision in *Virginia v. Black*, several courts use the "subjective test", which examines whether a reasonable speaker would foresee that the recipients of the communication would interpret it as threat.[83]

A "true threat" is a

---

[77] Op. cit., p. 385.

[78] See *RAV v. St. Paul.* (1992) 505 U.S. 377, 388, 22 June.

[79] *United States v. Jongewaard.* (2009) 567 F.3d 336, 340 (8th Cir.), 3 June.

[80] *United States v. Schweitzer.* (2017) No. 4: 17CR3094 (D. Neb.), 28 November.

[81] See *United States v. Parr.* (2008) 545 F.3d 491 (7th Cir.), 18 September.

[82] See, e.g. McCann, A.E. (2006) Are Courts Taking Internet Threats Seriously Enough? An Analysis of True Threats Transmitted Over the Internet, as Interpreted in United States v. Carmichael. *Pace Law Review*, 26, pp. 523, 527.

[83] *Virginia v. Black.* (2003) 538 U.S. 343, 360, 7 April (a "true threat" occurs where the *"speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death,"* without the need for the speaker to intend to carry out the threat).

> *"serious threat as distinguished from mere political argument, idle talk, or jest,"*
>
> *"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."*[84]

Also, a "true threat" is 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."*[85]

A threatening statement that is merely "hyperbole", or an exaggeration that aims to add a "heightened effect" to a certain viewpoint, without the intent to carry it out against a specific individual or property, is protected by the First Amendment and cannot be considered "true threat".[86] In *Commonwealth v. Knox*[87], for illustration, the court held that the "true threat" doctrine requires the speaker to have *"acted with an intent to terrorize or intimidate."*

In *United States v. Tinoco*[88], the defendant argued that his statements were not "true threats" as he

> *"didn't intend to place the victims in fear; (2) his Facebook posts didn't reach the victims; and (3) he frequently peppered his statements with the phrase 'figuratively speaking'."*

However, the court rejected the argument and held that, as the victim's testimony demonstrates, the threats were taken seriously (also, as per the defendant's own admission, according to which the people receiving his threats *"would feel threatened"*, and statements: *"I mean every word"* and *"You can quote me"*.)[89] Even if

---

[84] *United States v. Twitty.* (2019) Criminal Case No. 13-CR-00076-RBJ (D. Colo.), 4 January.

[85] *United States v. Parr.* (2008) 545 F.3d 491, 497 (7th Cir.), 18 September.

[86] *United States v. Kirsch.* (2015) 151 F. Supp. 3d 311, 313 (W.D.N.Y.), 16 December (*"Strong language that, if taken literally, may seem to communicate a threat, may not constitute a true threat"*).

[87] *Commonwealth v. Knox.* (2018) 190 A.3d 1146 (Pa.), 21 August.

[88] *United States v. Tinoco.* (2018) No. 17-2059 (10th Cir.), 28 March.

[89] Ibid.

> *"the alleged threat did not identify any specific person or group,"*

the defendant's communications can, in certain contexts, be interpreted as true threat.[90]

In *United States v. Killen*[91], the defendant posed as a young girl on a messaging-based mobile-phone application. The defendant sent to the victims images of a partially dressed girl and asked and received from the boys nude photos of themselves in return.[92] When the boys tried to end the contact with the defendant, the latter threatened the boys that, unless they will send him more nude photos, he will post the photos received on social media platforms, such as *Instagram*.[93] On appeal, the defendant challenged the sufficiency of the evidence.[94] However, taking into account the electronic evidence recovered from the defendant's electronic devices, and on the admission of the defendant to the extortionate conduct, the court found that there is

> *"sufficient evidence on these counts to permit a jury to find guilt beyond a reasonable doubt without testimony from the victims."*[95]

4.3. SENTENCING ASPECTS

The U.S.S.G., which contains non-binding rules that aim to create a uniform sentencing policy those convicted in the U.S. federal court system, has numerous enhancements that are applicable to these offenses. In *United States v. Sunmola*[96], for example, the defendant and his co-conspirators created profiles on dating websites, which included pictures of U.S. military men in uniforms as part of his online profile. After gaining the trust of women met online, the defendant and his co-conspirators asked for money and merchandise.[97] The defendant was charged with several offenses, including interstate extortion, in violation of 18 U.S.C. § 875(d). The defendant also sexually exploited the victims: he persuaded women to pose in a sexually suggestive positions, in front of a web camera. Without the victims' consent, the defendant recorded them, then posted the videos

[90] *United States v. Cox.* (1992) 957 F.2d 264, 266 (6th Cir.), 27 February.
[91] *United States v. Killen.* (2018) No. 15-15001 (11th Cir.), 29 March.
[92] Ibid.
[93] Ibid.
[94] Ibid.
[95] Ibid.
[96] *United States v. Sunmola.* (2018) 887 F.3d 830 (7th Cir.), 16 April.
[97] Ibid.

online and sent the relevant links to the victims and their relatives, with an extortion demand, containing the alarming warning that

"by the time he was finished with her she would want to kill herself."[98]

The court in this case applied the following sentencing enhancements: four-level leadership,[99] two-level for acting on behalf of a government agency,[100] four-level substantial financial hardship,[101] a two-level vulnerable victim,[102] a 16-level for an intended loss of $2,054,972.66,[103] and a two-level due to the perpetration of the offense outside of the United States.[104] The judge also granted two upward departures, for psychological injury to a victim and for the gratuitous infliction of injury to a victim.[105]

The defendant appealed the sentencing enhancements; however, the court held that the district court did not erred in imposing the enhancements, as follows, respectively: the defendant had a *"high level of control and authority"* in the scheme; while the defendant argued that he used the false military status

"to impress his victims, not for the purpose of obtaining a benefit on behalf of the military or other government organization,"

the court held that he misrepresented that he was acting on behalf of the military;[106] as per the findings in the *Pre-Sentencing Report (PSR)*, seven victims suffered substantial financial hardship, some of them submitted victim impact statements; while the victims were middle-aged women, rather than elderly, many of the women

---

98 *United States v. Sunmola.* (2018) 887 F.3d 830 (7th Cir.), 16 April, at 835.

99 U.S. Sentencing Commission. (2018) *Guidelines Manual*. Aggravating Role § 3B1.1(a). [online] Available from: https://guidelines.ussc.gov/gl/§3B1.1. [Accessed 4 June 2019].

100 U.S. Sentencing Commission. (2018) *Guidelines Manual*. Offense Conduct § 2B1.1(b)(9)(A). [online]. Available from: https://guidelines.ussc.gov/gl/§2B1.1. [Accessed 4 June 2019].

101 U.S. Sentencing Commission. (2018) *Guidelines Manual.* Offense Conduct § 2B1.1(b)(2)(B). [online]. Available from: https://guidelines.ussc.gov/gl/§2B1.1. [Accessed 4 June 2019] (the substantial financial hardship enhancement applies if the offense resulted in *"substantial financial hardship to five or more victims"*).

102 U.S. Sentencing Commission. (2018) *Guidelines Manual.* Hate Crime Motivation or Vulnerable Victim § 3A1.1(b)(1). [online]. Available from: https://guidelines.ussc.gov/gl/§3A1.1. [Accessed 4 June 2019].

103 U.S. Sentencing Commission. (2018) *Guidelines Manual.* Offense Conduct § 2B1.1(b)(1)(I). [online]. Available from: https://guidelines.ussc.gov/gl/§2B1.1. [Accessed 4 June 2019].

104 Ibid.

105 Op. cit., at 836.

106 Op. cit., at 838.

> *"had been divorced, abandoned, widowed, or ignored by the men in their lives"*

and, through online dating, they were seeking companionship, position that made them

> *"particularly susceptible to falling into the vicious trap of a man who deceitfully made them believe they were in love,"*

therefore vulnerable to extortionate tactics;[107] based on

> *"direct interviews, phone interviews, mailed-in statements, or mailed-in supporting documentation with the victims describing what happened and the amount of money they lost,"*

the determination of the total loss was construed as correctly calculated by the court.[108]

Another example of enhancements application, *United States v. Haileselassie*, the defendant appealed his sentence, which had two upward enhancements under the U.S.S.G. for *"substantial disruption of governmental function and obstruction of justice"*.[109] The appeal court, however, citing the

> *"extensive criminal history, including multiple convictions for threats, false reports, harassment, assault, trespass, and mailing threatening communications,"*

affirmed the sentence.[110] Other upward U.S.S.G. enhancements applicable to these offenses include substantial disruption of governmental function and obstruction of justice,[111] violation of court protective orders, making of multiple threats, and intention to carry out the threats.[112]

---

[107] Op. cit., at 837.
[108] Op. cit., at 840.
[109] *United States v. Haileselassie.* (2019) No. 18-1343 (8th Cir.), 10 June.
[110] Ibid.
[111] Ibid.
[112] *Irizarry v. United States.* (2008) 553 U.S. 708, 128 S. Ct. 2198, 171 L. Ed. 2D 28, 12 June.

4.4. THE INSANITY DEFENSE

Cyber extortion and threats are specific intent crimes, allowing defendants to bring up defenses involving their mental or emotional conditions.[113] Importantly, however, insanity is a legal, not a medical aspect.[114]

Evidence of a defendant's mental problems at the time of the crime is brought up to establish the insanity defense. This defense, however,

> *"is not concerned with the mens rea element of the crime; rather, it operates to completely excuse the defendant whether or not guilt can be proven."*[115]

Different from "insanity", the diminished capacity defense, which regards a defendant's ability to come to the required criminal state of mind, is not considered an excuse:

> *"successful defendants simply are not guilty of the offense charged, although they are usually guilty of a lesser included offense."*[116]

As explained by the court in *United States v. Long*, a severe mental disease or defect (such as the schizotypal personality disorder) alone, will not be considered enough for the purposes of 18 U.S.C. § 17(a), which regards the affirmative defense of insanity:

> *"there must be sufficient evidence of a temporal and causal nexus between the symptoms of the disease and the commission of the acts themselves."*[117]

However, the defendants that have a mental disease or defect, can, upon receiving treatment, be rendered competent to stand the trial. In *United States v. Arega*, for instance, the defendant was charged with transmitting a threatening communication.[118] After a *"regimen of medications, including antipsychotics,"* the medical evaluation rendered the defendant as being lucid, no longer suffering

---

[113] *United States v. Sullivan.* (2016) No. 3: 13-cr-00064-HZ (D. Or.), 6 January.

[114] See *Kahler v. Kansas.* (2020) No. 18-6135 (U.S.), 23 March (*"The insanity defense sits at the juncture of medical views of mental illness and moral and legal theories of criminal culpability."*); The Free Dictionary. *Insanity Defense*. [online]. Available from: https://legal-dictionary.thefreedictionary.com/Insanity+Defence [Accessed 2 July 2019] (*"A defense asserted by an accused in a criminal prosecution to avoid liability for the commission of a crime because, at the time of the crime, the person did not appreciate the nature or quality or wrongfulness of the acts."*).

[115] *United States v. Twine.* (1988) 853 F.2d 676, 678 (9th Cir.), 1 August.

[116] Op. cit., at 678.

[117] *United States v. Long.* (2009) No. 07-31131 (5th Cir.), 5 March.

[118] *United States v. Arega.* (2018) No. 1: 17-cr-00225-TSC (D.C.), 17 January.

> *"from the irrational and delusional ideation that he had previously exhibited,"*

therefore competent to stand the trial.[119]

In *United States v. Christian*[120], the defendant, charged with two counts of transmitting, via e-mail, threats to injure the person of another, in violation of 18 U.S.C. § 875(c), in order to establish that he was incapable of forming the specific intent to threaten, raised the diminished capacity defense. The district court, however, precluded his expert witness from testifying.[121] *The Court of Appeals*, held that the district court acted abusively by not considering the expert's testimony, which could have helped the jury decide on the defendant's capacity

> *"to form the specific intent to threaten when he sent the emails at issue,"*

and vacated and remanded the conviction for a new trial.[122]

United States v. Ivers provides another example of mental competency examination: the defendant was charged with transmission of threats to assault and murder a law enforcement officer, in violation of 18 U.S.C. § 115(a)(1)(B) and 18 U.S.C. § 875(c).[123] During the initial competency hearing, the defendant, who claimed that

> *"federal authorities (he most commonly names the CIA and FBI) implanted a 'non organic foreign body/object' into his brain and had been using the implant to torture him,"*

was not found competent to stand the trial, as he was assessed to suffer *"from mental disease or defect,"* therefore not mentally competent

> *"to understand the nature and consequences of the proceedings against him or to assist properly in his defense."*[124]

---

[119] Ibid.
[120] *United States v. Christian.* (2014) 749 F.3d 806-8 (9th Cir.), 17 April.
[121] Op. cit., at 809.
[122] Op. cit., at 811–5.
[123] *United States v. Ivers.* (2018) No. 3: 16-cr-00347-AA (D. Or.), 21 February.
[124] Ibid.

After several months of hospitalization, the clinical psychologist assessed that the defendant can communicate in a "'very rational' manner" and can stand the trial.[125]

Mental diseases or defects can also be taken into consideration for reduced sentences. In *United States v. Humphries*, for illustration, the defendant experienced

> *"symptoms consistent with diagnosis of Post-Traumatic Stress Disorder (PTSD), Obsessive Compulsive Disorder (OCD) and adjustment disorder with mixed anxiety and depressed mood."*[126]

Taking the defendant's mental issues into consideration, the court granted a downward departure from the U.S.S.G. In contrast, in *United States v. Wyrick*, the defendant-appellant, contested as "substantively unreasonable" his 37-month sentence for the numerous telephone calls containing threats to injure the person of another he made, in violation of 18 U.S.C. § 875(c). The defendant-appellant cited his diagnosed mental condition of "Delusional Disorder, Persecutory and Erotomania Type" and his "true first offender" status, and requested a downward sentencing variance.[127] The appeal court found that a downward variance, based on the defendant's mental illness, was unwarranted, as the defendant's behavior

> *"was no less serious as a result and is no less likely to happen again."*[128]

The appeal court went on and, while it acknowledged the defendant's arguments, considered them *"unconvincing given the facts of the case"* and affirmed the sentence of the district court.[129]

5. CONCLUSION

This article presented a comprehensive analysis of the cyber extortion and threats phenomenon. The article extends the understanding of the phenomenon by providing a thorough understanding

[125] Ibid (the defendant was administered the Inventory of Legal Knowledge and the MacArthur Competence Assessment Tool-Criminal Adjudication).

[126] *United States v. Humphries.* (2013) No. 12 Cr. 347 (RWS) (S.D.N.Y.), 28 October.

[127] *United States v. Wyrick.* (2011) No. 10-3117 (10th Cir.), 24 March (people suffering from Delusional Disorder-Erotomania Type *"believe another person, usually someone of a higher social status, is in love with them"*).

[128] Ibid.

[129] Ibid.

of the attributes and of the most important litigation aspects, such as the legal elements of these offenses, how the U.S. legal system addresses them, and sentencing aspects.

The article evidenced that these communications, especially in their extreme forms, can have very serious consequences, such as placing the victims in an constant state of fear and stress, which can result in a major psychological harm or generalized trauma, disrupting the course of people's activities, and affecting public interests.

The phenomenon poses complex and many-faceted challenges regarding the criminalization, prosecution, and sentencing. For a more effective response to this phenomenon, it is necessary to better understand the initiation and escalation of these offenses, to form threat assessment professionals, and to promote law enforcement best practice guidelines. There is also a need for stronger and more coherent legal framework, including uniform interpretation of the legal elements of these offenses and the explicit incrimination of intentional infliction of emotional distress. Appropriate protection of personally identifying information, including through encryption and redaction, must also receive adequate consideration.

The development of effective computerized natural language analysis tools, employed to analyze the linguistic features of the phenomenon, can help better control the phenomenon, by filtering out of such communications, triggering account termination, and referring such instances to law enforcement, for a prompt reaction to imminent threats.

General educational programs that address related aspects, such as cyberviolence risks, personal data protection, preservation of digital evidence, appropriate reactions to cyber threats, and incident reporting, can also play a significant role in the control of the phenomenon.

Even though this article analyzed cases from just one jurisdiction, the findings can be of interest to a global audience. The findings of this article can be used to elaborate educational materials for law enforcement training programs and for law school clinics, to develop fact analysis and client advising skills.

LIST OF REFERENCES

[1] Barney, D. (2016) Elonis v. United States: Why the Supreme Court Punted on Free Speech. *Pepperdine Law Review*, 2016.

[2] Berman, M.N. (1998) The Evidentiary Theory of Blackmail: Taking Motives Seriously. *University of Chicago Law Review,* 65.

[3] Brusco, M.A. (2016) Read This Note or Else!: Conviction Under 18 U.S.C. § 875(c) for Recklessly Making a Threat. *Fordham Law Review*, 84.

[4] Bumb, M. L. (2017) Domestic Violence Law, Abusers' Intent, and Social Media: How Transaction-Bound Statutes Are the True Threats to Prosecuting Perpetrators of Gender--Based Violence. *Brooklyn Law Review*, 82 (2).

[5] Coenen, D.T. (2017) Freedom of Speech and the Criminal Law. *Boston University Law Review*, 97.

[6] Collins, E. (2018) Insane: James Holmes, Clark v. Arizona, and America's Insanity Defense. *Journal of Law and Health*, 31.

[7] *Commonwealth v. Knox.* (2018) 190 A.3d 1146 (Pa.), 21 August.

[8] Crump, D. (2010) What Does Intent Mean? *Hofstra Law Review*, 38.

[9] Cybercrime Convention Committee (T-CY). (2018) *Mapping Study on Cyberviolence*. [online] Strasbourg: Council of Europe.

[10] *Elonis v. United States.* (2015) 135 S. Ct. 2001, 575 U.S., 192 L. Ed. 2D 1, 1 June.

[11] European Institute for Gender Equality. (2017) *Cyber violence against women and girls*.

[12] European Union Agency for Law Enforcement Cooperation (Europol). (2017) *Internet Organised Crime Threat Assessment*. The Hague: Europol.

[13] Florida Statutes 836.05 Threats; extortion.

[14] *Fontana v. United States.* (2020) No. 14-20141 (E.D. Mich.), 17 April.

[15] Geha, G. (2016) Think Twice Before Posting Online: Criminalizing Threats Under 18 U.S.C. § 875(c) After Elonis. *John Marshall Law Review*, 50.

[16] Green, S.P. (2005) Theft by Coercion: Extortion, Blackmail, and Hard Bargaining. *Washburn Law Journal*, 44.

[17] Han, D.S. (2014) The Mechanics of First Amendment Audience Analysis. *William and Mary Law Review*, 55.

[18] Harawa, D.S. (2014) Social Media Thoughtcrimes. *Pace Law Review*, 35.

[19] *In the Matter of Search of a Residence in Oakland.* (2019) Case No. 4-19-70053 (N.D. Cal.), 10 January.

[20] *Irizarry v. United States.* (2008) 553 U.S. 708, 128 S. Ct. 2198, 171 L. Ed. 2D 28, 12 June.

[21] Kachulis, L. (2017) Insane in the Mens Rea: Why Insanity Defense Reform is Long Overdue. *Southern California Interdisciplinary Law Journal*, 26.

[22] *Kahler v. Kansas.* (2020) No. 18-6135 (U.S.), 23 March.

[23] McCann, A.E. (2006) Are Courts Taking Internet Threats Seriously Enough? An Analysis of True Threats Transmitted Over the Internet, as Interpreted in United States v. Carmichael. *Pace Law Review*, 26.

[24] Peterson, J. and Densley, J. (2017) Cyber Violence: What Do We Know and Where Do We Go From Here?. *Aggression and Violent Behavior*, 34.

[25] Pierce, M. (2015) Prosecuting Online Threats After Elonis. *Northwestern University Law Review*, 110.

[26] Quek, J.X. (2016) Elonis v. United States: The Next Twelve Years. *Berkeley Technology Law Journal*, 31.

[27] *RAV v. St. Paul.* (1992) 505 U.S. 377, 388, 22 June.

[28] Roark, M.M. (2015) Elonis v. United States: The Doctrine of True Threats: Protecting Our Ever-Shrinking First Amendment Rights in the New Era of Communication. *Pittsburgh Journal of Technology Law & Policy*, 15.

[29] Romney, J. (2012) Eliminating the Subjective Intent Requirement for True Threats in United States v. Bagdasarian. *Brigham Young University Law Review*, 2012.

[30] *Scheidler v. National Organization for Women.* (2003) 537 U.S. 393.

[31] Shavell, S. (1993) An Economic Analysis of Threats and Their Illegality: Blackmail, Extortion, and Robbery. *University of Pennsylvania Law Review,* 141.

[32] Spitzberg, B.H. and Gawron, J.M. (2016) Toward Online Linguistic Surveillance of Threatening Messages. *Journal of Digital Forensics, Security and Law*, 11.

[33] Strasser, M. (2011) Advocacy, True Threats, and the First Amendment. *Hastings Constitutional Law Quarterly*, 38.

[34] The Free Dictionary. *Insanity.*

[35] *United States v. Abrahams.* (2013) No. 8:13-mj-00422 (C.D. Cal.), 17 September.

[36] *United States v. Alkhabaz.* (1997) 104 F.3d 1492 (6th Cir.), 29 January.

[37] *United States v. Arega.* (2018) No. 1: 17-cr-00225-TSC (D.C.), 17 January.

[38] *United States v. Avenatti.* (2020) No.(S1) 19 Cr. 373 (PGG) (S.D.N.Y.), 14 January.

[39] *United States v. Bagdasarian.* (2011) 652 F.3d 1113 (9th Cir.), 19 July

[40] *United States v. Bishop.* (2018) Case 118MJ24LDA (D.R.I.), 23 January.

[41] *United States v. Cain.* (2018) No. 1: 16-cr-00103-JAW (D. Me.), 1 June.

[42] *United States v. Carrillo.* (2020) No. 1: 19-cr-01991 KWR (D.N.M.), 8 April.

[43] *United States v. Champ, United States v. Wood.* (2006) 459 F. Supp. 2d 451 (E.D. Va.), 29 September.

[44] *United States v. Chansler.* (2010) No. 3:10-cr-00100 (M. D. Fla.), 15 April.

[45] *United States v. Christian.* (2014) 749 F.3d 806-8 (9th Cir.), 17 April.

[46] *United States v. Christy.* (2019) No. 3: 18-CR-223 (M.D. Pa.), 14 February.

[47] *United States v. Coss.* (2012) 677 F.3d 278 (6th Cir.), 16 April.

[48] *United States v. Cox.* (1992) 957 F.2d 264, 266 (6th Cir.), 27 February.

[49] *United States v. Cruz.* (2017) No. 15-3139 (3d Cir.), 8 November.

[50] *United States v. Dillard.* (2011) 835 F. Supp. 2d 1120 (D. Kan.), 21 December.

[51] *United States v. Doggart.* (2020) 947 F.3d 879 (6th Cir.), 15 January.

[52] *United States v. Dutcher.* (2017) 851 F.3d 757 (7th Cir.), 22 March.

[53] *United States v. Fontana.* (2017) No. 16-2208 (6th Cir.), 15 August.

[54] *United States v. Fowler.* (2010) Case No. 8:10-cr-65-T-24 AEP (M.D. Fla.), 25 October.

[55] *United States v. Gillenwater.* (2014) 749 F.3d 1094 (9th Cir.), 11 April.

[56] *United States v. Gomez.* (2020) No. 18-12089 (11th Cir.), 14 February.

[57] *United States v. Gossett.* (2019) No. 1: 19-cr-00081 WJ (D.N.M.), 7 May.

[58] *United States v. Haileselassie.* (2019) No. 18-1343 (8th Cir.), 10 June.

[59] *United States v. Heineman.* (2014) 767 F.3d 970, 972 (10th Cir.), 15 September.

[60] *United States v. Humphries.* (2013) No. 12 Cr. 347 (RWS) (S.D.N.Y.), 28 October.

[61] *United States v. Ivanov*. (2001) 175 F. Supp. 2d 367 (D. Conn.), 6 December.

[62] *United States v. Ivers.* (2018) No. 3: 16-cr-00347-AA (D. Or.), 21 February.

[63] *United States v. Jongewaard.* (2009) 567 F.3d 336, 340 (8th Cir.), 3 June.

[64] *United States v. Jordan.* (2017) No. 16-CR-93-FPG-HKS-1 (W.D.N.Y.), 24 October.

[65] *United States v. Kadar.* (2017) Case No. 6:17-mj-1361 (M.D. Fla.), 4 April.

[66] *United States v. Killen.* (2018) No. 15-15001 (11th Cir.), 29 March.

[67] *United States v. Kirsch.* (2015) 151 F. Supp. 3d 311, 313 (W.D.N.Y.), 16 December.

[68] *United States v. Leach.* (2017) Case No. 2:17mj-44-1 (D. Vt.), 21 April.

[69] *United States v. Lisnyak.* (2015) Case No. 15-04179MJ-PCTDMF (D. Ariz.), 16 July.

[70] *United States v. Long.* (2009) No. 07-31131 (5th Cir.), 5 March.

[71] *United States v. McCrudden.* (2015) No. CR-11-061 (DRH) (E.D.N.Y.), 16 March.

[72] *United States v. Michael.* (2012) No. 2: 12-cr-1-WTL-CMM (S.D. Ind.), 9 October.

[73] *United States v. Parr.* (2008) 545 F.3d 491 (7th Cir.), 18 September.

[74] *United States v. Petrovic.* (2012) 701 F.3d 849 (8th Cir.), 13 December.

[75] *United States v. Schweitzer.* (2017) No. 4: 17CR3094 (D. Neb.), 28 November.

[76] *United States v. Smith.* (2017) 878 F.3d 498 (5th Cir.), 28 December.

[77] *United States v. Springer.* (2018) No. 17-15584, Non-Argument Calendar (11th Cir.), 26 October.

[78] *United States v. Sullivan.* (2016) No. 3: 13-cr-00064-HZ (D. Or.), 6 January.

[79] *United States v. Sunmola.* (2018) 887 F.3d 830 (7th Cir.), 16 April.

[80] *United States v. Swarbrick.* (2018) Case 3:18-MJ-1214 (M.D. Tenn.), 19 September.

[81] *United States v. Telfair.* (2020) No. 19-CR-270 (E.D.N.Y.), 3 February.

[82] *United States v. Tinoco.* (2018) No. 17-2059 (10th Cir.), 28 March.

[83] *United States v. Turrella.* (2012) No. 10-30051 (9th Cir.), 15 March.

[84] *United States v. Twine.* (1988) 853 F.2d 676, 678 (9th Cir.), 1 August.

[85] *United States v. Twitty.* (2019) Criminal Case No. 13-CR-00076-RBJ (D. Colo.), 4 January.

[86] *United States v. Vandevere.* (2019) No. 1: 19-cr-63-MOC (W.D.N.C.), 16 September.

[87] *United States v. Wheeler.* (2015) 776 F.3d 736, 743 (10th Cir.), 15 January.

[88] *United States v. Wheeler.* (2019) Criminal Case No. 12-cr-0138-WJM (D. Colo.), 9 July.

[89] *United States v. White.* (2010) Criminal Action No. 7:08-CR-00054 (W.D. Va.), 20 January.

[90] *United States v. White.* (2017) Criminal Action No. 7: 13CR00013 (W.D. Va.), 31 May.

[91] *United States v. Williams.* (2012) 693 F.3d 1067 (9th Cir.), 7 September.

[92] *United States v. Williams.* (2018) No. 17-2454 (8th Cir.), 26 October.

[93] *United States v. Wyrick.* (2011) No. 10-3117 (10th Cir.), 24 March.

[94] U.S. Department of Justice. (2010) *Prosecuting Computer Crimes*. [online] Washington: Office of Legal Education Executive Office for United States Attorneys.

[95] U.S. Departmentt of Justice. (2016) *The National Strategy for Child Exploitation Prevention and Interdiction*.

[96] U.S. Model Penal Code.

[97] Van Der Wilk, A. (2018) *Cyber violence and hate speech online against women*. PE 604.979. Brussels: European Parliament.

[98] *Virginia v. Black.* (2003) 538 U.S. 343, 360, 7 April.

[99] Volokh, E. (2016) The Freedom of Speech and Bad Purposes. *UCLA Law Review*, 63.

[100] *White v. United States.* (2019) No. 6: 17-cv-689-Orl-28GJK (M.D. Fla.), 14 February.

[101] Women and Gender Equality Canada. (2019) *New federal investment will help end cyberviolence*. [press release] 27 August. Available from: https://www.canada.ca/en/status-women/news/2019/08/new-federal-investment-will-help-end-cyberviolence.html [Accessed 3 December 2019]