Article

Journal of Contemporary Criminal Justice
1–22

DOI: 10.1177/10439862211001590
journals.sagepub.com/home/ccj
SAGE

Institutional Anomie Theory and Cybercrime—Cybercrime and the American Dream, Now Available Online

Thomas E. Dearden[1], Katalin Parti[1], and James Hawdon[1]

Abstract

As the world becomes increasingly connected and interdependent upon technology, crimes are moving online. Research on cybercrime is beginning to test the applicability of traditional criminological theories for understanding crime in this new medium. Using a national sample of 215 self-admitted cybercriminals, we examine Messner and Rosenfeld's institutional anomie theory. Negative binomial regressions reveal that expressed levels of institutional anomie correlate with increased cybercrime activity. A curvilinear relationship was found, such that low and high levels of institutional anomie lead to higher levels of cybercrime. Our findings reveal how the dark side of the American Dream can lead to online criminality. Specifically, the penetration of, and accommodation to economic values dictated by American capitalism can lead individuals to adopt values such as the fetishism of money that, in turn, affects their online behavior and criminality.

Keywords

strain, institutional anomie, noneconomic institutions, cybercrime, cybercriminology

Our world is becoming increasingly connected through technology. From social media to online shopping, we live in the age of the internet. Cisco estimates that currently there are more than eight networked devices per person in the United States, and this number is expected to climb to more than 13 devices per person by 2022

[1]Virginia Tech, Blacksburg, USA

Corresponding Author:
Katalin Parti, Assistant Professor of Sociology, Virginia Tech, 560 McBryde Hall (0137), 225 Stanger Street, Blacksburg, VA 24061, USA.
Email: kparti@vt.edu

(Cisco, 2020). We use computers to socialize, communicate, work, and play. Yet, these technological connections also increase opportunities for new types of committing crimes that are facilitated by computers and the internet. Some of these crimes include hacking, online fraud, identity theft, spamming, and cyberbullying (Ngo & Jaishankar, 2017). Not surprisingly, as the world becomes more dependent on cyberconnections, cybercrime is increasing (Jardine, 2015). According to Gallup, 23% of households in America were victims of hacking to personal, credit card, or financial information, and an additional 16% of households were victims of identity theft. These rates of victimization surpass those reported for street crimes, where only 11% were victims of vandalism, 3% of houses were broken into, and 4% of individuals were physically assaulted, robbed, or sexually assaulted (Reinhart, 2018).

Given the widespread nature of cybercrime and the costs it can entail, there is an obvious need to better understand its causes and consequences. Although an impressive body of literature has now investigated patterns of cybercrime victimization, far fewer studies have been able to study the perpetrators of cybercrimes. The relatively limited number of studies that have examined cybercriminals often test the applicability of a traditional criminological theory as a potential explanation for the cybercrime in question. We provide another such examination by offering what we believe is the first application of Messner and Rosenfeld's (1994/2003) institutional anomie theory (IAT) to a variety of cybercrimes. The goal of the study is to examine whether the overemphasis on economic goals results in higher rates of cybercriminal behavior. In other words, whether those who display any one of the four values—achievement, individualism, universalism, and the fetishism of money—of Messner and Rosenfeld's theory, are more likely to engage in any cybercriminal activity

Strain Theory and Cybercrimes

Various criminological theories have been used to explain different types of cybercrimes. The most frequently used crime theories to explain cybercrime besides routine activities (Bossler & Holt, 2009; Holt & Bossler, 2009; Reyns, 2013) are self-control (Donner et al., 2014; Reyns et al., 2019), social learning theory (Hawdon et al., 2019; Holt et al., 2010), and general strain theory (GST; Patchin & Hinduja, 2011).

Strain theory has been applied to acts of hacking, piracy, online scams, cyberstalking/harassment, and online hate speech (Chism & Steinmetz, 2018). Merton's influential theory on social structure and anomie (1938) described crime as the result of the differential access to legitimate, institutionally defined means to achieve culturally defined goals, especially monetary success. American culture emphasizes the pursuit of the American Dream. This dream involves the pursuit of money to access the all-encompassed desire for material objects such as car, house, and an overall well-being. However, despite this culturally defined goal, the institutionally determined means fail to provide equal opportunities for all members of society to achieve it. Deviant adaptations occur when an individual abandons the desired goal, the legitimate means to achieve the goal, or both. Merton's strain theory, although criticized, has been extremely influential and gone through numerous revisions (e.g.,

GST, IAT). These revised versions of strain theory have been widely applied to offline crimes with varying levels of success; however, the application of strain theory to cybercrimes is limited.

To date, there is a limited body of research that considers cybercrime from a strain theory perspective. Larsson et al. (2012) explain digital piracy as an innovation to achieving goals, as well as the innovation of virtual private networks (VPNs) that provides anonymity. Cyber political activist can also be explained with strain theory as they "actively construct new environments that offer new means—file-sharing platforms, anonymization tools" to achieve their goals (Larsson et al., 2012, p. 108, cited by Yar & Steinmetz, 2019, p. 31). Agnew's GST, which posits that criminal acts are performed as an attempt to cope with negative emotions such as depression, anxiety, and anger that result strain (Agnew, 1992), has also been applied to cybercrime. Most of the research using GST focuses on cyberbullying and harassment (Hay & Meldrum, 2010; Patchin & Hinduja, 2011; Wright & Li, 2012). According to these researchers, cyberbullying can be both a stressor (source) and a strain-releasing strategy (outcome or by-product) of digital harassment. Yet, the support for GST for explaining cybercrime is limited. For example, Hay et al. (2010) found experiencing cyberbullying victimization as a source of strain was a weak predictor of self-harm and suicidal ideation. Similarly, other forms of cyber deviance such as music piracy do not seem to be a significant outcome of strain (Hinduja, 2006, 2012).

Institutional Anomie and the American Dream

Derived from Durkheim's (1897/1987) discussion of anomie and Merton's (1968, 1938) strain theory, Messner and Rosenfeld's IAT (1994/2013) explains crime on a macro level. Specifically, crime rates are a function of cultural pressures to achieve economic goals, that is, the American Dream. The American Dream, according to these theorists, refers to a commitment to the goal of material success, to be pursued by everyone, under conditions of open, individual competition. Four values permeate the American dream: achievement at any cost, intensive individualism, universalism (everyone should succeed), and the fetishism of money (Messner & Rosenfeld, 1994/2003, pp. 62–65). Thus, achievement is valued, an individual should achieve it by herself or himself, everyone should succeed, and success is defined solely through monetary means.

Although these cultural goals do not directly lead to crime in and of themselves, they do lead to the widespread pursuit of economic success within an anomic culture and an environment where the behavioral controls from noneconomic institutions such as the family or polity have been weakened. The development of American capitalism and adoption of the American Dream have resulted in noneconomic institutions being ineffective at exercising control over the pursuit of economic success via any means, including criminal means (Messner & Rosenfeld, 1994/2013). This supremacy of the economic institution over all other institutions has occurred through the *devaluation* of noneconomic institutional functions (e.g., education is merely a means to money), *accommodation* to economic requirements by other institutions (e.g., family routines

are dominated by work schedules), and *penetration* of economic norms into other institutional domains (e.g., politics are based on the "bottom line"). It is the intensive pursuit of economic success combined with an "anomic ethic" and insufficient institutional controls that lead to widespread criminal activity. Despite being originally developed with a focus on the United States, IAT likely applies to other developed, western nation-states with disembedded economies (see Bernburg, 2002; Chamlin & Cochran, 2007; Hagan et al., 1998).

In addition to recognizing that IAT may apply to other developed capitalist economies, theorists have also introduced an individual-level component to the theory: marketized mentality (Groß et al., 2018; Hövermann et al., 2016; Hövermann, Groß, et al., 2015; Hövermann, Messner, et al., 2015). Marketized mentality is a strong individual commitment to values and role performance repertoires (or the lack of them) that contribute to institutional anomie. Karstedt and Farrall (2006) further explicated the individual component of IAT by studying "crimes of everyday life" (Karstedt & Farrall, 2006, p. 1011). They coined the term "market anomie," which represented a general lowered level of trust in others in the marketplace, fear of victimization when being involved in business, and legal cynicism. All of these values were determinants of involvement in crimes.

The Empirical Status of IAT

Most empirical evaluations of IAT have examined the additive and multiplicative effects of the structural antecedents of the institutional imbalance of power and anomie on violent (e.g., Piquero & Piquero, 1998; Savolainen, 2000) and property crime rates (e.g., Chamlin & Cochran, 1995). Although largely limited to the United States, these studies have generally been supportive of IAT. Studies examining the cross-national applicability of IAT, although limited in number, have found modest support for the theory. Zito (2018) using data from the World Values Study and a multilevel model, found that rule violation is more readily accepted by those in anomic market societies. Individuals in countries with more economic freedom but less economic equality and countries where money fetishism is accepted are more supportive of individual rule breaking. Contrastingly, individuals in countries with strong noneconomic institutions such as family and polity were less likely to justify rule breaking. Individual financial difficulties, weaker social institutions, economic inequality, and high levels of individualism were all associated with justifications of everyday criminal activity (for an overview, see Hövermann & Messner, 2019). Dolliver (2013) also found that cultural–institutional configurations vary between countries and groups of countries, and each configuration differentially affected organized crime in Europe; however, homicide rates (i.e., the traditional dependent variable that has been used in the majority of past empirical studies of IAT) did not conform well to the theory's predictions (Dolliver, 2013).

Passas (2000) observes that globalization and neoliberalism reproduce structural problems typical of anomie, as neoliberal economies fail to deliver their promises, just like American capitalism. According to Passas (2000), global

interconnectedness, economic growth, free markets, individualism, consumerism, privatization, and deregulation of neoliberal markets have created new needs. However, structural asymmetries in economy, law, politics, and culture aggravate the divergence between means and ends, thereby producing a sense of deprivation and frustration in those who fail to achieve the globally valued goals of success (Passas 2000). Such strains can induce deviance (Passas, 2000), such as global crime, as a result of the combination of anomic states (remote cause) and individual and situational criminogenic factors (proximate causes).

Other researchers testing solely the more individualized component of IAT have generally found support for this version of the theory (e.g., Muftic, 2006; Rosenberger, 2016; Stults & Falco, 2014; Tuliao & Chen, 2017). For example, Muftic (2006) studied cheating prevalence in college students, and found that measures associated to economic goals of the American Dream such as individualism, universalism, achievement orientation, and "monetary fetishism" (i.e., marketized values), and level of commitment to noneconomic institutions such as family and polity, influence cheating. Both those who showed adherence to the marketized values and those less committed to family and polity were more likely to cheat (Muftic, 2006). Others (e.g., Hirtenlehner et al., 2013; Kittleson, 2012), however, found less support in a cross-national setting. Perhaps because of the homogeneous culture of European countries, neither economic dominance, nor weakened noneconomic institutions, nor individual cultural values predicted individual crime proneness among Europeans. After introducing the individual sociopsychological measure of "marketized mentality," Hövermann and colleagues (Hövermann, Groß, et al., 2015; Hövermann, Messner, et al., 2015) found associations between "egoistic individuality" and money fetishism (the metric of success), dictated by the universal economic need of monetary success (Messner, 2003).

Although IAT has enjoyed reasonable empirical success at the macro and micro levels, it has not yet been widely applied to cybercrimes. Although several studies test the influence of strain on cybercrime (Chism & Steinmetz, 2018; Hay et al., 2010; Hay & Meldrum, 2010; Hinduja, 2006, 2012; Larsson et al., 2012; Patchin & Hinduja, 2011; Wright & Li, 2012), few tests of IAT in cyberspace exist (Muftic, 2006). The current study attempts to fill that gap by evaluating the applicability of the theory on the commission of deviant activities in cyberspace.

Additional Considerations

The factors identified by IAT have generally been assumed to be linearly related to criminal behavior, and this has certainly been the logic behind the more micro version of the theory. However, there is reason to suspect that the relationship may be curvilinear. It is likely that very low levels of the individual-level components of the theory could be related to crime, at least to some extent. Harkening back to Mertonian strain theory, those who rejected the culturally defined goals and the institutionally defined means corresponded to the mode of adaptation Merton referred to as to use a retreatism (Merton, 1938). Although this mode of adaptation was allegedly related to such

deviant acts as drug use or skid row alcoholics, it can also be related to such cybercrimes as hacking, especially hacktivists or others who reject the basic tenets of the American Dream (e.g., Jordan & Taylor, 2004). Then, at modest levels of IAT, it is likely that the criminal behavior may actually decrease or at least be less related to criminality than it is at higher levels. Indeed, other theories find that commitment to traditional goals is inversely related to crime (e.g., Hirschi, 1969). The American Dream has served as a strong motivator for individuals to achieve material success through hard work, as has been widely argued by its proponents and even echoed by then candidate for the U.S. Senate, Barak Obama, in his 2004 keynote address to the Democratic National Convention (Obama, 2004; see Rowland & Jones, 2007, for a discussion). It is when these values reach extremes that they become criminogenic (Merton, 1938). Thus, we anticipate that the relationship between IAT values and cybercrime will be U-shaped as low levels of IAT will be weakly but positively related to crime, more moderate levels of IAT will become unrelated or inversely related to crime, and then the relationship between IAT and cybercrime will be far stronger at the highest levels of IAT than it is at lower levels. We now turn to our empirical test.

Method

Sample

Data were collected between November 24 and 29, 2019, from a Dynata panel. Dynata uses random digit dialing, banner ads, and other permission-based techniques to recruit potential respondents. They then randomly selected panel members who received invitations to participate in the survey. The sample was demographically balanced to represent the U.S. population in terms of sex, ethnicity, and race. In total, 1,315 respondents began the survey; however, 81 (6.2%) were identified as speeders and eliminated from the analyses and 125 (9.5%) did not complete the first question and were also eliminated from the analyses. In total, usable data were collected from 1,109 (84.3%) respondents.

Online proportional sampling panels demographically balanced on important population characteristics such as sex, race, and ethnicity have been found to yield similar results as random probability-based samples (Simmons & Bobo, 2015; Weinberg et al., 2014; although MacInnis et al., 2018, offers a differing perspective). Demographically balanced panels ensure one-time participation through IP address matching and eliminate speeders through attention checks and mean-time comparisons with the overall sample (Evans & Manthur, 2005; Wansink, 2001). Moreover, prepanel interviews and participation incentives increase participant interest and the overall response validity of the overall data (see Wansink, 2001).

The sample was 49.7% female, 73.4% White, 15.0% Black or African American, 6.0% Asian, and 2.1% American Indian or Alaskan Native. Slightly more than 17% of the sample identified as Hispanic. These numbers closely match the U.S. population and are well within the expected margin of error for a sample of 1,109 (U.S. Census Bureau, 2019).

Table 1. Self-Reported Offending Behavior.

Types of offending behavior	Respondents who reported engaging in past 12 months		% of total self-reported offenders (n = 215[a])
	Count	% of total sample (n = 1,109)	
Posted hurtful information about someone on the internet	101	9.16	47.00
Threatened or insulated others through email or instant messaging	89	8.08	41.40
Excluded someone from an online community	117	10.61	54.42
Hacked into an unauthorized area of the internet	71	6.44	33.02
Distributed malicious software	60	5.44	27.91
Illegally downloaded copyrighted files or programs	100	9.09	46.51
Illegally uploaded copyrighted files or programs	76	6.90	35.35
Used someone else's personal information on the internet without their permission	68	6.17	31.63
Bought prescriptions (without a prescription) or other drugs on online pharmacies or websites	80	7.27	37.21
Posted nude photos of someone else without his or her permission	67	6.09	31.16

[a]Add up to more than 100% as each offender can commit more than one offense.

Measures

Dependent variable. Our dependent variable included self-reported participation in several cyber-offending behaviors during the 12 months preceding the survey. The counts of each offending behavior are found in Table 1.

We combined the binary responses of each offending behavior to create a general index of cyber offending. For this new general cyber-offending variable, the minimum value was 0, indicating no offending behavior within the 12 months prior to completing the survey, and the maximum was 10, indicating a self-report of all offending behaviors within the 12 months preceding the survey. It is worth noting that of all participants who reported cyber-offending behaviors (n = 215), only 36% (n = 78) reported only one offending behavior. All others reported two or more cyber offenses. Figure 1 shows the distribution of the cyber-offending variable.

Although not traditionally utilized to examine binary data, a correlation matrix of offending behaviors can help us understand which behaviors are more likely to overlap. The highest R values, indicating the highest overlap in offending, included the distribution of malicious software and uploading copyrighted content (r = .67) and sending threatening messages and posting nudes of someone without their permission (r = .66). The lowest overlap in offending included downloading copyrighted content and buying drugs online (r = .44) and identity theft and excluding someone from online communities (r = .46).

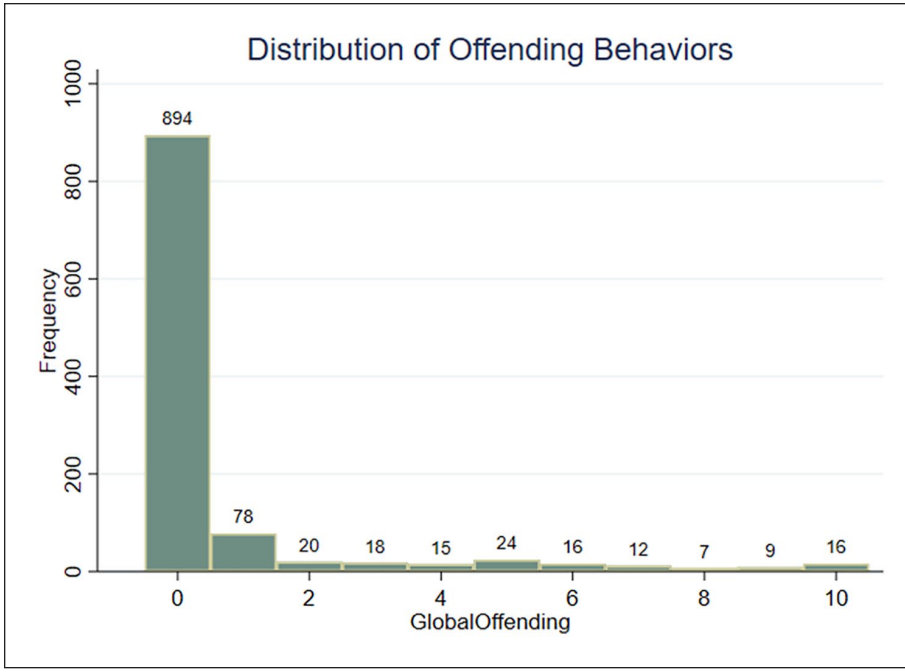

Figure 1. Past 12-month self-report offending counts.

Independent variables. The primary independent variable of interest was an individual-level scale of IAT. Descriptive statistics for each question are presented in Table 2. Muftic's (2006) original scale taps six subscales: Individualism, Achievement (second set of four questions), Universalism, Fetishism of Money, Family, and Education. Although this original scale included 23 items, the full scale was not available in these data. The available items were from the Individualism (first four questions in Table 2), Achievement (second set of four questions), and Fetishism of Money (last three questions) subscales. We investigated whether these items loaded onto the corresponding subscales, but the analysis indicated that a one-factor solution fit the data well. We therefore combined these items into a general IAT index by summing each question ($\alpha = .883$). To test for the curvilinear effect, we suspect may exist between IAT and cyber offending, we also created the quadratic term of the IAT. The data were centered before creating the quadratic as suggested in the literature (e.g., Aiken & West, 1991).

Control variables. Other common variables used in analyses of cybercrime include measures related to routine activities. We measured variables related to computer knowledge and time spent on the dark web. These were both measured ordinally. Computer knowledge was measured with a Guttman-like scale. Respondents were asked "how familiar are you with computers," and responses included "I am

Table 2. IAT Questions.

IAT question	*M*	*SD*	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
Being successful is more important than being happy (n = 1,083)	1.18	1.16	0.36	0.29	0.21	0.1	0.05
I intend to do whatever it takes to have some of the really expensive things in life (n = 1,078)	1.29	1.2	0.35	0.23	0.24	0.14	0.04
I expect to make as many sacrifices as are necessary to advance my work/career (n = 1,083)	1.56	1.17	0.25	0.22	0.31	0.18	0.04
I expect to devote whatever time and energy it takes to move up in my job/career (n = 1,081)	1.71	1.22	0.22	0.19	0.3	0.22	0.07
Success is measured by the amount of money a person makes (n = 1,081)	1.32	1.22	0.35	0.21	0.25	0.14	0.05
I am getting/have gotten an education because it is expected by my friends or parents (n = 1,077)	1.67	1.25	0.25	0.19	0.29	0.2	0.08
I will sacrifice a lot of other things to have a lot of money (n = 1,081)	1.39	1.21	0.31	0.23	0.27	0.14	0.05
I do not need help from others to succeed (n = 1,079)	1.73	1.16	0.18	0.25	0.31	0.2	0.06
Having lots of money is one of my major goals in life (n = 1,080)	1.75	1.26	0.22	0.19	0.29	0.21	0.09
Education is only helpful to get a good job (n = 1,080)	1.75	1.26	0.21	0.23	0.26	0.21	0.1
Education is useful because it helps you make more money (n = 1,079)	2.36	1.09	0.08	0.12	0.28	0.4	0.12

Note. IAT = institutional anomie theory.

uncomfortable using a computer"; "I can 'surf the net,' use common software, but not fix my computer problems"; "I can use a variety of software and fix some of my computer problems"; "I can use a variety of operating systems and fix most computer problems I have"; and "I am comfortable manipulating or writing computer programming." To measure time spent on the dark web, respondents were asked "how many hours per week do you spend on the dark web," and responses included 0 hr, less than 1 hr, 1 to 2 hr, 2 to 4 hr, 4 to 6 hr, 7 to 10 hr, and 10 hr or more. In addition, we have included a control for general trust, which was a 5-point Likert-type item for the statement, "how much do you trust people in general."

In addition, a series of demographic and control variables were included to better understand the effect of IAT on offending. These variables are shown in Table 3. The demographic variables include gender, age measured as a continuous variable, and race (see Table 3 for categories). In addition, education was measured by asking respondents what is the highest level of education they achieved, and the responses included "less than a high school diploma," "a high school degree," "some college," "a college degree," or "a master's degree, professional degree or higher." Household income was measured by asking what the combined income of all members in your household was in the last year, and the categories are reported in Table 3. Descriptive statistics for all variables are presented in Table 3.

Regression models. Several models were run to better understand the effect of individual levels of IAT on general cyber offending. As cyber offending, the dependent variable, was a count variable (i.e., an index of binary responses to specific cyber offending in the past 12 months) and because the data were significantly overdispersed, negative binomial regressions were utilized. These models are similar to regression, in that, they allow for correlations to be established but are appropriate for count data (Long & Freese, 2005).

In the first negative binomial regression, cyber offending was regressed on the overall IAT index to examine the independent relationship between IAT and cyber offending. IAT was positively related to the commission of cybercrimes ($b = .056$, incidence-rate ratio [IRR] = 1.07, $p < .001$). The risk of committing a cybercrime increase by approximately 7% for every increase of 1 on the IAT scale. In the second model, we introduce the quadratic term of IAT. This was done to consider the curvilinear relationship between IAT and cyber offending. We hypothesized that both low levels and high levels of IAT would relate to cyber offending. A linear model would not capture this relationship and so a squared term was introduced to allow the model to account for a curvilinear model. Here, both IAT ($b = .048$, $p < .001$) and IAT^2 ($b = .003$, $p < .001$) were statistically significant, thereby indicating a curvilinear relationship between IAT and cyber offending (see Figure 2). As predicted, as IAT is extremely low, its relationship with offending is relatively weak; however, as IAT increases, we see a progressively higher likelihood of cyber offending.

The next model considered all covariates with the general index of IAT and the quadratic term for IAT. This model was done to understand the multivariate relationship between IAT and cyber offending by using the control variables mentioned

Table 3. Control Variable Descriptive Statistics.

Gender	Male	Female	LGBTQ+/nonbinary				
	548 (50%)	531 (49%)	16 (1%)				
Education	Less than high school	High school	Some college	College degree	MA/professional/PhD		
	32 (3%)	236 (21%)	265 (24%)	387 (35%)	187 (17%)		
Race	White	Black	American Indian	Asian	Pacific Island/ Hawaiian	Other/prefer not to answer	
	789 (71%)	157 (14%)	13 (1%)	70 (6%)	9 (1%)	71 (6%)	
Household income	<US$25k	US$25k–US$50k	US$50k–US$75k	US$75k–US$100k	US$100k–US$150k	US$150k–US$250k	>US$250k
	189 (18%)	273 (26%)	174 (17%)	179 (17%)	138 (13%)	70 (7%)	26 (2%)
Age	Mean	Median	*SD*	Min	Max		
	42	42	13.68	18	80		
Time spent on dark web (hours per week)	0	<1	1–2	2–4	4–6	7–9	10 or more
	706 (74%)	49 (5%)	47 (5%)	37 (4%)	43 (5%)	32 (3%)	42 (4%)
Computer knowledge	Uncomfortable	Surf net	Software to fix computer	Fix and use multiple OS	Able to write code		
	93 (8%)	307 (28%)	379 (35%)	209 (19%)	111 (10%)		
How much do you trust people in general	A great deal	A lot	A moderate amount	A little	None at all		
	78 (7%)	148 (13%)	460 (42%)	316 (28%)	104 (9%)		

Note. LGBTQ = lesbian, gay, bisexual, transgender, and queer; OS = operating system.

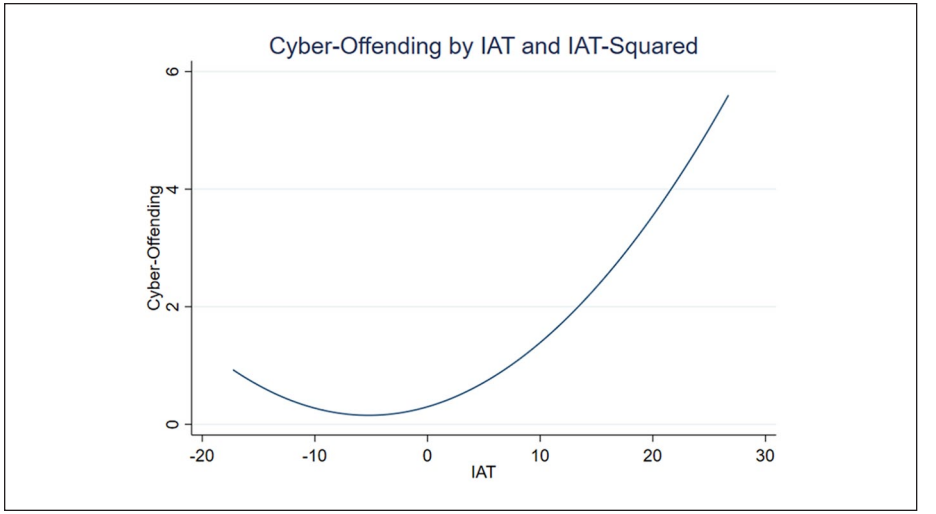

Figure 2. Curvilinear effect of IAT on cyber offending.
Note. IAT = institutional anomie theory.

above. As shown in Table 4, the overall model was statistically significant ($p < .001$), and the main effect of IAT was statistically significant using traditional standards ($b = .01$, $p < .001$). Most interestingly, the IAT quadratic term remains significant ($b = .002$, $p < .001$). Once again, we see that IAT and cyber offending is curvilinearly related, even after controlling for other relevant factors. Other significant variables included an increase in cyber offending for both Blacks ($b = .660$, $p = .009$) and Asians ($b = .828$, $p = .010$) compared with Whites; a decrease in cyber offending as age increases ($b = -.047$, $p < .001$), an increase in cyber offending as dark web use increases ($b = .336$, $p < .001$), and an increase in cyber offending as general trust decreases ($b = -.298$, $p = .001$).

Discussion

Overall, we found that IAT correlates with self-reported online offending behavior. In all three models, IAT was a significant predictor of cyber offending. Although pseudo-R^2 is not comparable with R^2 and should be interpreted with caution (Long & Freese, 2005), our pseudo-R^2 ranged from .02 for the base IAT model to .14 for the full model including covariates. Our findings suggest that IAT is correlated with cyber offending and future studies should continue to examine and include this theory as a part of criminological explanations.

More important than significant findings for the IAT model, we found a strong curvilinear effect when using IAT^2 as a predictor. Overall, extremely low levels of IAT and high levels of IAT relate to cyber offending. This is an important discovery in our study and for the theory generally. With mixed support for IAT in the literature

Table 4. Poisson Regressions Predicting Cyber-Offending Index.

	IAT				IAT^2				Full model			
Variable	*B*	*SE* (*B*)	*p*	IRR	*B*	*SE*(*B*)	*p*	IRR	*B*	*SE*(*B*)	*p*	IRR
IAT	0.056	.008	***	1.06	0.048	.010	***	1.05	0.026	.026	**	1.03
IAT^2					0.003	.001	***	1.00	0.002	.001	***	1.00
Gender (ref.: male) Female									−0.277	.19		0.76
LGBTQ+									1.029	.64		1.80
Education									−0.050	.106		0.95
Race (ref.: White)												
Black									0.660	.253	***	1.93
Asian									0.828	.321	**	2.29
American Indian									0.964	.804		2.62
Pacific Islander									−0.173	.902		0.84
Income									0.117	.068		1.12
Age									−0.047	.007	***	0.95
Dark web									0.336	.052	***	1.40
Familiarity									−0.096	.075		0.91
Trust									−0.298	.093	***	0.74
Constant	−492	.058	***	0.61	−0.850	.118	***	0.43	0.890	.570		2.43
Pseudo R^2		.02				.03				.14		
LR χ^2		43				63				218		

Note. IAT = institutional anomie theory; IRR = incidence-rate ratio; LGBTQ = lesbian, gay, bisexual, transgender, and queer; LR X^2 = Likelihood Ratio chi-square.
*$p < .1$. **$p < .05$. ***$p < .01$.

(Messner et al., 2019), a curvilinear effect can help explain these mixed findings. Furthermore, we believe that this effect fits conceptually within the theory. Although the theoretical notions focus on increased IAT relating to crime, an argument that rejecting the American Dream (i.e., having a very low IAT) would also be related to crime. If one has too much apathy toward the capitalistic values illustrated in IAT, then perhaps there is no reason to buy into the market system at all. Instead, crime could be used as a path of least resistance or convenient way to survive. This notion is explicitly stated in Merton's (1938) strain theory, as he argued that the rejection of culturally defined goals results in the modes of adaptation of either retreatism or ritualism. Whereas ritualism is unlikely to result in criminal behavior because the institutionally defined means are accepted, retreatism would be correlated with crime, according to Merton (1938). Moreover, this notion that failing to adopt culturally defined goals as a contributing factor to criminal behavior is also surely expressed in control theories, such as social bonding theory (Hirschi, 1969).

The curvilinear effect suggests that the relationship between IAT and crime is complex. Individuals who engage too little with notions of the American Dream or other market anomie ideas are more likely to engage in crime. The same can be said of those who adhere to these notions too much. However, there does appear to be an adherence where individuals are engaged with market ideas and values but not to an excessive point. Perhaps what is occurring at the high end is that individuals are prioritizing success at all costs, leading to the breaking of rules or laws to achieve. This would certainly be consistent with the original notions of anomie. Here, goals are themselves not bad, but the prioritization of financial or market success at the cost of all other goals may lead individuals to discount moral elements in favor of economic success.

Other significant predictors of cybercrime included gender, race, age, dark web use, and trust. To better understand the relationship with gender, we considered the overall offending rate. Overall, females offended in 18% of our sample, whereas males offended in 22%.

Consistent with findings on age and crime, we found that as age increases cybercrime decreases. This may be even more pronounced for cybercrime as historical stereotypes have considered cybercrimes, such as hacking, to be conducted primarily by juveniles (Yar, 2005).

Race differences were also found, such that Blacks and Asians reported a higher rate of offending than did Whites. When we look at specific cybercrimes, interesting patterns emerge. Although not statistically significant, Blacks and Asians are more likely than Whites to report online harassment, exclusion, online threats, illegal copyright download, and revenge pornography, which supports the findings of hate crime literature underlining the role that race and ethnicity play in hate speech online (Williams et al., 2020). Notably but unexpectedly, as the pattern does not fit the relatively high-level involvement in hate-related interpersonal crime in these populations, African American and Asian participants also scored fairly high on hacking.

We also found that dark web use is positively correlated with increased cybercrime activity. This was not surprising as some cybercrimes, including digital piracy and drug sales, are frequently conducted on the dark web (Hurlburt, 2017).

We were surprised to find that computer familiarity was not significantly related to cybercrime. And, if anything, as familiarity increased, cybercrime decreased ($p. = .204$). This relationship should be further explored as some cybercrimes are facilitated by greater computer literacy. For example, whereas cybercrimes such as online bullying require very little computer skill, hacking can require considerable skills. It could be by combining all types of cybercrime, the effect of computer knowledge is muddied. Although we could conceivably test for a curvilinear effect in our model, we refrained from doing so because it is beyond the scope of our main objective of testing IAT's utility for explaining cybercrime. However, we briefly examined this possibility using *t* tests with specific cybercrimes. We found marginal support for this notion as those who reported hacking reported higher computer skills ($t = -1.66$, $n = 1{,}143$, $p = .010$), whereas those who reported posting hurtful information were not significantly different compared with the general sample on computer skills ($t = 0.6$, $n = 1{,}142$, $p = .58$).

In terms of education's relationship with cyber offending, the model suggests offending decreases as education increases, but this effect fails to achieve statistical significance ($p = .637$). The relationship between education and cybercrime may be too complex to detect using linear models, much like computer familiarity. Some crimes may require more education, though this does not need to be a formal progression through grades as is commonly measured. Conversely, other cybercrimes may require little education or skill.

This article shows the American adult population's involvement in a variety of cybercrime activities on a small, yet nationally representative, sample. Institutional anomie is inflicted by radical and rapid socioeconomic change, which generates social problems that push the limits of the market economy to the point that it cannot cope adequately. This refers to the current situation in the United States, with the country undergoing significant economic and sociopolitical changes, as well as serious political debates concerning traditional democratic institutions (Fukuyama, 2014; Gilens & Page, 2014). These changes have recently taken a rapid pace, resulting in an increased level of anomie (Gupta & Gupta, 2018) and a decrease in the positive effects of strong social institutions such as the family, state, and community.

If these changes were not enough, institutions of social cohesion, such as education and health care, have been witnessing reforms for years. These changes increase uncertainty, difficulties in prospecting whether socially approved success scenarios such as earning high levels of education and working hard will lead to monetary success and save people from debts. The vicious cycle becomes complete when financial inequality and negative socioeconomic change meet with social and financial inequalities. The economic equality on the macro level together with money fetishism on the individual level creates tremendous pressures on individuals to succeed at all costs. This constellation is rather supportive of individual rule breaking. The commission of cybercrime by both those who are the most and the least affected by institutional anomie supports the above-described tenet of IAT.

The media historically portray the computer criminal as a smart but reclusive youth (Alper, 2014). We believe that our models show a different characterization of cyber

offending. Including a broader range of online illegal behaviors shows that computer knowledge is not related to offending. Adding the findings on IAT and trust supports that offenders are more defined by their beliefs than their demographics. For example, someone high on IAT may recognize the strong market presence online and utilize the internet, in sophisticated or unsophisticated ways, to scam individuals out of money or private information. Similarly, another individual low on IAT may recognize the convenience of buying illegal drugs or downloading copyrighted material off the internet. Although a speculation at this point, further research should examine specific types of cybercrimes and behaviors related to IAT.

IAT does not offer easy prescriptive solutions to fixing crime. Instead, we see a culmination of market forces overtaking alternative goals. Thus, we see that offline behavior and forces are influencing online behavior and computer cyber offending. We add our voice to the sociological chorus suggesting that an overvaluation of market goals is contributing to criminal behavior through overvaluation (e.g., financial achievement at all costs). We also suggest that the same forces are contributing to crime through undervaluation and "checking out" (e.g., deciding, consciously or unconsciously, that financial achievement is impossible, and no other achievement is worthwhile).

Limitations

Using an online survey inherently includes several limitations. First, our ability to detect causal relationships was limited. The regressions performed merely show that IAT is correlated with cyber offending. Future work should consider experimental or quasi-experimental designs to examine these processes in time order or longitudinally to clearly establish the temporal order of the variables. Moreover, longitudinal surveys could also be designed to consider changes of over time.

Although our initial sample included more than 1,100 participants, we were largely working with a sample of 215. This was because we focused only on cyber offending. The population of cyber offenders is inherently difficult to target, and as such we had to include a large sample to reach these 215. Thus, we utilized a subset of the data, which only yields 1,100 participants.

One concern with any data collection effort is that participants may lie. Although this is always a possibility, we found evidence that showed consistency among responses. For example, when considering the overlap of offending behaviors, we found the strongest correlations between the distribution of malicious software and uploading copyrighted content ($r = .67$). These behaviors have a strong correlation in the real world as including malicious code or viruses in uploaded content is relatively common (Federal Trade Commission, 2019). Similarly, we found strong correlations between sending threatening messages and posting nude images of someone without their permission ($r = .66$). It is unsurprising that these behaviors correlate given their likely connection with online aggression and their similarly low sophistication. Thus, if participants lied about their offending, then they did so in a way that appears to be consistent with what we would expect of online offenders.

Because of the low number of certain populations in our sample, some results of our survey must be interpreted with caution. For example, the observed relationships between race/ethnicity and cybercrime should be considered with due caution, and how these relationships play out in connection with IAT should be studied in the future.

Conclusion and Implications

This article analyzes IAT as it correlates to crimes committed online. Overall significant effects were found such that higher and lower levels of IAT were correlated with increased self-reports of cyber offending. While providing evidence of IAT's utility in explaining cybercrime, we believe that other micro-level factors, such as the social learning process, techniques of neutralization, and social reinforcement, should also be considered to identify the complexity of components of victimization and offending online. This would serve toward the creation of a general cyber-integrated theory of crime (Bossler, 2020).

Although the literature measuring IAT's effect on cybercrime is scarce (Donner et al., 2014; Reyns et al., 2019), our study is a significant addendum to the existing literature as it proves that IAT affects cybercriminal activity of a national sample of the adult American population. We recommend further studying IAT's effect on cybercrime in different populations, including other developed, as well as developing countries.

The present article examines individual factors of cybercrime by studying the effect of IAT on cyber offenders. However, for obvious reasons, it does not look at cybercrime as a global phenomenon. The combination of the anomic state (remote cause) and individual and situational criminogenic factors (proximate causes of cybercrime; Passas, 2000) must be examined in the future, as cybercrime is a global phenomenon.

In recent years, many jurisdictions all over the world have adopted cybersecurity strategies. These strategies generally ignore cybercriminal motivations and adapt their cybersecurity plans on the sole measure of intrusion detection (Pasculli, 2020). Therefore, there is a need to improve our understanding of cybercrime causes to assess and, if necessary, reform existing strategies, calculating with individual motivations. Our recommendation is to further study IAT and its effects on individual motivations of cybercriminal activity in the future.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was funded by the Center for Peace Studies and Violence Prevention at Virginia Tech (Grant number 025-19); The Institute for Culture,

Society, and Environment at Virginia Tech; and The Integrated Security Destination Area at Virginia Tech.

ORCID iDs

Thomas E. Dearden https://orcid.org/0000-0003-0549-927X

Katalin Parti https://orcid.org/0000-0002-8484-3237

James Hawdon https://orcid.org/0000-0002-0273-2227

References

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47–88.

Aiken, L., & West, S. (1991). *Multiple regression: Testing and interpreting interactions*. SAGE.

Alper, M. (2014). "Can our kids hack it with computers?" Constructing youth hackers in family computing magazines (1983-1987). *International Journal of Communication*, *8*(1), 673–698.

Bernburg, J. G. (2002). Anomie, social change, and crime: A theoretical examination of institutional-anomie theory. *British Journal of Criminology*, *42*, 729–742.

Bossler, A. (2020). Contributions of criminological theory to the understanding of cybercrime offending and victimization. In R. Leukfeldt & T. Holt (Eds.), *The human factor of cybercrime* (pp. 29–59). Routledge.

Bossler, A., & Holt, T. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

Chamlin, M. B., & Cochran, J. K. (1995). Assessing Messner and Rosenfeld's institutional anomie theory: A partial test. *Criminology*, *33*, 411–429.

Chamlin, M. B., & Cochran, J. K. (2007). An evaluation of the assumptions that underlie institutional anomie theory. *Theoretical Criminology*, *11*(1), 39–61.

Chism, K. A., & Steinmetz, K. F. (2018). Strain theory and technocrime. In K. F. Steinmetz & M. R. Nobles (Eds.), *Technocrime and criminological theory*. (pp. 66–84). Routledge.

Cisco. (2020). *Cisco visual networking index: Forecast and trends, 2018–2023* [White Paper]. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html#_Toc532256789

Dolliver, D. S. (2013). *Organized crime, culture, and social institutions in Europe: An application of institutional anomie theory* [Unpublished PhD dissertation]. Northeastern University.

Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior*, *34*, 165–172.

Durkheim, E. (1987). *Suicide: A study in sociology* (J. A. Spaulding & G. Simpson, Trans.). Routledge & Kegan Paul. (Original work published 1897).

Evans, J., & Manthur, A. (2005). The value of online surveys. *Internet Research*, *15*(2), 195–219.

Federal Trade Commission. (2019). *Malware from illegal video streaming apps: What to know*. Federal Trade Commission Consumer Information. https://www.consumer.ftc.gov/blog/2019/05/malware-illegal-video-streaming-apps-what-know

Fukuyama, F. (2014). America in decay. The sources of political dysfunction. *Foreign Affairs*, *93*(1), 5–26.

Gilens, M., & Page, B. I. (2014). Testing theories of American politics: Elites, interest groups, and average citizens. *Perspectives on Politics*, *12*(3), 564–581.

Groß, E. M., Hövermann, A., & Messner, S. F. (2018). Marketized mentality, competitive/egoistic school culture, and delinquent attitudes and behavior: An application of institutional anomie theory. *Criminology*, *56*(2), 333–369.

Gupta, K., & Gupta, S. (2018). Durkheim's theory of anomie and the 2016 American election. *Journal of Global Economy*, *14*(1), 28–39.

Hagan, J., Hefler, G., Classen, G., Boehnke, K., & Merkens, H. (1998). Subterranean sources of subcultural delinquency beyond the American dream. *Criminology*, *36*(2), 309–342.

Hawdon, J., Bernatzky, C., & Costello, M. (2019). Cyber-routines, political attitudes, and exposure to violence-advocating online extremism. *Social Forces*, *98*(1), 329–354.

Hay, C., & Meldrum, R. (2010). Bullying victimization and adolescent self-harm: Testing hypotheses from general strain theory. *Journal of Youth and Adolescence*, *39*, 446–459.

Hay, C., Meldrum, R., & Mann, K. (2010). Traditional bullying, cyberbullying, and deviance: A general strain theory approach. *Journal of Contemporary Criminal Justice*, *26*(2), 130–147.

Hinduja, S. (2006). *Music piracy and crime theory*. LFB Scholarly.

Hinduja, S. (2012). General strain, self-control and music piracy. *International Journal of Cybercriminology*, *6*(1), 951–967.

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

Hirtenlehner, H., Farrall, S., & Bacher, J. (2013). Culture, institutions, and morally dubious behaviors: Testing some core propositions of the institutional-anomie theory. *Deviant Behavior*, *34*(4), 291–320.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1–25.

Holt, T. J., Burrus, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31–61.

Hövermann, A., Groß, E. M., & Messner, S. F. (2016). Institutional imbalance, integration into noneconomic institutions, and a marketized mentality in Europe: A multilevel, partial elaboration of institutional anomie theory. *International Journal of Comparative Sociology*, *57*(4), 231–254.

Hövermann, A., Groß, E. M., Zick, A., & Messner, S. F. (2015). Understanding the devaluation of vulnerable groups: A novel application of institutional anomie theory. *Social Science Research*, *52*, 408–421.

Hövermann, A., & Messner, S. F. (2019). Institutional imbalance, marketized mentality, and the justification of instrumental offenses: A cross-national application of institutional anomie theory. *Justice Quarterly* Advance online publication. https://doi.org/10.1080/07418825.2019.1590621

Hövermann, A., Messner, S. F., & Zick, A. (2015). Anomie, marketization, and prejudice toward purportedly unprofitable groups. *Acta Sociologica*, *58*(3), 215–231.

Hurlburt, G. (2017). Shining light on the dark web. *Computer*, *50*, 100–105.

Jardine, E. (2015). *Global cyberspace is safer than you think: Real trends in cybercrime* (Global Commission on Internet Governance Paper Series, No, 16). https://www.cigionline.org/sites/default/files/no16_web_0.pdf

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and cyberwars: Rebels with a cause?* Routledge.

Karstedt, S., & Farrall, S. (2006). The moral economy of everyday crime. *The British Journal of Criminology*, *46*(6), 1011–1136.

Kittleson, M. (2012). *A cross-national, longitudinal test of institutional anomie theory* [Master's thesis]. Western Michigan University. http://scholarworks.wmich.edu/masters_theses/54

Larsson, S., Svensson, M., & Kaminski, M. (2012). Online piracy, anonymity, and social change. *Convergence: An International Journal of Research into New Media Technologies*, *19*(1), 95–114.

Long, J. S., & Freese, J. (2005). *Regression models for categorical dependent variables using Stata*. Stata Press.

MacInnis, B., Krosnick, J. A., Ho, A. S., & Cho, M. J. (2018). The accuracy of measurements with probability and nonprobability survey samples: Replication and extension. *Public Opinion Quarterly*, *82*(4), 707–744.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review*, *3*, 672–682.

Merton, R. K. (1968). *Social Theory and Social Structure*. Free Press.

Messner, S. F. (2003). An institutional-anomie theory of crime: Continuities and elaborations in the study of social structure and anomie. *Cologne Journal of Sociology and Social Psychology*, *43*, 93–109.

Messner, S. F., & Rosenfeld, R. (2013). *Crime and the American Dream* (5th ed.). Wadsworth. (Original work published 1994).

Messner, S. F., Rosenfeld, R., & Hövermann, A. (2019). *Institutional anomie theory: An evolving research program*. Springer International. https://doi.org/10.1007/978-3-030-20779-3_9

Muftic, L. (2006). Advancing institutional anomie theory: A microlevel examination connecting culture, institutions, and deviance. *International Journal of Offender Therapy and Comparative Criminology*, *50*(6), 630–653.

Ngo, F., & Jaishankar, K. (2017). Commemorating a decade in existence of the international journal of cyber criminology: A research agenda to advance the scholarship on cybercrime. *International Journal of Cyber Criminology*, *11*(1), 1–9.

Obama, B. (2004). *Keynote address to the Democratic National Convention*. https://www.pbs.org/newshour/show/barack-obamas-keynote-address-at-the-2004-democratic-national-convention

Pasculli, L. (2020). The global causes of cybercrime and state responsibilities. Towards an integrated interdisciplinary theory. *Journal of Ethics and Legal Technologies*, *2*(1), 48–75.

Passas, N. (2000). Global anomie, dysnomie, and economic crime: Hidden consequences of neoliberalism and globalization in Russia and around the world. *Social Justice*, *27*(2), 16–44.

Patchin, J. W., & Hinduja, S. (2011). Traditional and non-traditional bullying among youth: A test of general strain theory. *Youth & Society*, *43*(2), 727–751.

Piquero, A., & Piquero, N. L. (1998). On testing institutional anomie theory with varying specifications. *Studies on Crime and Crime Prevention*, *7*, 61–84.

Reinhart, R. J. (2018). *One in four Americans have experiences cybercrime.* Gallup Politics. https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238.

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice*, *44*(1), 63–82.

Rosenberger, J. S. (2016). Television consumption and institutional anomie theory. *Sociological Focus*, *49*(4), 305–325.

Rowland, R. C., & Jones, J. M. (2007). Recasting the American dream and American politics: Barack Obama's keynote address to the 2004 Democratic National Convention. *Quarterly Journal of Speech*, *93*(4), 425–448.

Savolainen, J. (2000). Inequality, welfare state, and homicide: Further support for the institutional anomie theory. *Criminology*, *38*, 1021–1042.

Simmons, A. D., & Bobo, L. D. (2015). Can non-full-probability internet surveys yield useful data? A comparison with full-probability face-to-face surveys in the domain of race and social inequality attitudes. *Sociological Methodology*, *45*(1), 357–387.

Stults, B. J., & Falco, C. S. (2014). Unbalanced institutional commitments and delinquent behavior. *Youth Violence and Juvenile Justice*, *12*(1), 77–100.

Tuliao, K. V., & Chen, C.-W. (2017). Economy and supervisors' ethical values: Exploring the mediating role of noneconomic institutions in a cross-national test of institutional anomie theory. *Journal of Business Ethics*, *156*, 823–838.

U.S. Census Bureau. (2019). https://www.census.gov/quickfacts/fact/table/US/RHI125218#RHI125218

Wansink, B. (2001). Editorial: The Power of Panels. *Journal of Database Marketing & Customer Strategy Management*, 8(3), 190–194.

Weinberg, J. D., Freese, J., & McElhattan, D. (2014). Comparing data characteristics and results of an online factorial survey between a population-based and a crowdsource-recruited sample. *Sociological Science*, *1*, 292–310.

Williams, M. L., Burnap, P., Javed, A., Liu, H., & Ozalp, S. (2020). Hate in the machine: Anti-Black and anti-Muslim social media posts as predictors of offline racially and religiously aggravated crime. *The British Journal of Criminology*, *60*(1), 93–117.

Wright, M. F., & Li, Y. (2012). Kicking the digital dog: A longitudinal investigation of young adults' victimization and cyber-displaced aggression. *Cyberpsychology, Behavior and Social Networking*, *15*(9), 448–454.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Criminal Justice*, *44*(4), 387–399.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE.

Zito, R. C. (2018). Institutional anomie and justification of morally dubious behavior and violence cross-nationally: A multilevel examination. *Australian & New Zealand Journal of Criminology*, *52*(2), 250–271.

Author Biographies

Thomas E. Dearden is assistant professor of sociology at Virginia Tech. He specializes in research technology and crime and corporate crime. He has published his research in peer-reviewed journals including *The Journal of Financial Crime* and *The Journal of Investigative Psychology and Offender Profiling* and has presented at a dozen different conferences.

Katalin Parti is assistant professor of sociology at Virginia Tech. Her research focuses on cybercrime and online bullying. She has published in peer-reviewed journals such as the *Pediatrics*, the *International Journal of Cybersecurity Intelligence & Cybercrime*, the *European Journal of Crime Criminal Law and Criminal Justice*, and the *Journal of Contemporary European Research.*

James Hawdon is a professor of sociology and director of the Center for Peace Studies and Violence Prevention at Virginia Tech. He researches on how communities influence the causes and consequences of violence. He has been funded by the National Science Foundation, the National Institute of Justice, the National Consortium on Violence Prevention, and several other agencies. He has published or edited eight books and more than 100 articles and technical reports.