## Unit 8: Digital Deviance

**Welcome to Week 8.**
This week's learning explores a very difficult question: why individuals commit cyberspace crimes. This is an important question, because the answer(s) might affect the way this crime is dealt with. You will evaluate whether traditional criminological theories can explain this sort of deviance, or whether there is need to rethink our understanding of the reasons why people engage in cyber harmful activities.

**On completion of this unit you will be able to:**

- Explore issues concerning digital deviance.
- Assess the extent criminological theories can make sense of cyberspace deviance.
- Practice research skills.
- Apply evaluation skills.

**Reflection:**
**Deviance** refers to the violation of social conventions. People have varying conceptions of what sorts of acts might be deemed deviant, making it difficult to accurately characterize.

Cybercrime and Digital Deviance addresses cybercrimes such hacking and romance scams, as well as cyberdeviant behaviors like pornography addiction, trolling, and flaming. Sociology, criminology, and computer science are the sources for the material offered in this study. Other themes covered include cybercrime investigations, organized cybercrime, the use of algorithms in law enforcement, cybervictimization, and the theories used to explain cybercrime (Graham & Smith, 2019).

**Possibile outcomes of deviation include both positive and negative deviance.**

**Negative deviance:**

- The definition of negative deviance is behavior that does not conform to the established norms.
- Negative deviants oppose the norms, have a warped perception of the norms, or are ignorant of the norms.

**Positive deviance:**

- Over-adherence to standards is a type of positive deviance. Positive deviants attempt to improve the community's norms.
- Positive deviance can be equally challenging to govern and destructive as negative deviance.

**The Nature of Deviance:**
Sociologists consider a deviant a person who has violated one or more of the standards that are held in the greatest regard by society.

Typical negative responses to deviants typically involve efforts to change or otherwise influence the deviant's behavior.

**What are some of the unintended repercussions of deviation?**

- Deviance erodes confidence.
- Deviance has the power to inspire others' nonconformity.
- The price of deviant behavior is costly.

**What beneficial impacts does divergence have on society?**

- To safeguard its values, a community builds, modifies, and confirms its norms through the act of exercising social control. Norms are thereby clarified.
- Deviance has the capacity to serve as a temporary safety valve.
- Deviance can actually bring together members of a group or organization.
- Deviance is a vital catalyst for important societal transformation.

**Internet Facilitates Crime and Deviance in cyberspace**

Cybercrimes are crimes performed using networked technologies (Wall, 2007). Cyberspace and modern information technologies have spawned new expressions of crimes such as theft, fraud, and harassment that are centuries old. Other crimes, including as hacking and internet-based prostitution solicitation, are examples of contested deviance. Considerable subgroups view actions as neither aberrant nor outside the range of acceptable moral norms. Statistics on cybercrime from industry security systems, for example, may overestimate the prevalence of hacking since they may contain low-level automated attacks that do not impact functionality or steal data (Wall, 2007). In addition, ransomware, malware, and worms are frequently produced as forms of resistance against unfair government or company regulations. However, there is no consensus regarding the criminalization of types of hacking.

By making alternative motives and normative perspectives on various forms of cybercrime more visible and accessible, the Internet facilitates the commission of aberrant behavior and illegal action. The fragmented and layered character of the Internet further encourages deviant and criminal behavior due to the absence of a centralized government entity to establish standards of acceptable behavior and enforce criminal laws in specific countries. Since the Internet is a worldwide network, this is the case. Offenders can select locations for their websites with the least severe legal repercussions by taking advantage of the fact that some nations condone criminal behavior while others regard it as legitimate. In addition, it is easier for criminals to conduct crimes in virtual spaces while hiding behind false identities or remaining anonymous than it would be in the real world. Apps, avatars, disposable devices, and the deep web — an area of the internet where search engines cannot discover websites due to an additional layer of security — make it easier for individuals engaging in illegal or unusual behavior to conceal their financial transactions, socialize within underground communities, and network with like-minded individuals**. Cyberspace's specialized forums** and chat rooms have enabled virtual venues for networking and the formation of reputable underground markets for illegal substances, prostitution, and child pornography (Beech, et. al., 2008; Lavorgna, 2014; Stalans & Finn, 2016). These virtual forums have also allowed ideologically aberrant organizations to encourage terrorism, conduct espionage, and engage in harmful health hazards such as "bug chasing" (Frederick & Perrone, 2014; Rediker, 2015). These forums allow for global outreach, the construction of vendors' reputations through customer reviews, the discussion of evasive methods to escape arrest, and the creation of market norms that discourage law enforcement collaboration (Lavorgna, 2014). The pervasiveness of information technology and cyberspace in the interconnection of things such as automobiles, telephones, home security systems, and home temperature controls, as well as its role as critical infrastructure for societal institutions, highlights the potential for serious and damaging effects associated with cybercrime.

**Cybercriminology** is an interdisciplinary topic that combines computer science, psychology, sociology, criminology, and other fields to examine how and why people commit various forms of cybercrime, as well as the real-world implications of these crimes. Although the field is still in its infancy, cybercrime research on a wide variety of types has already begun to accumulate. This includes book collections that contain international research (Wall, 2007) as well as two reviews of the present state of knowledge in the topic. The role of the Internet and technology in dating violence has been reviewed (Stonard, et. al., 2014), as well as the online grooming behavior of child sex offenders and child pornography (Stonard, et. al., 2014). Other evaluations have evaluated the current level of knowledge regarding why offenders commit various online cybercrimes not covered in the general reviews (Beech et al., 2008). In recent years, the primary focus of the area has been on applying well-established criminological theories to specific and different operationalizations of various types of cybercrime, such as hacking, online fraud, and online harassment. The subject of whether cybercrimes are essentially classic crimes committed in new contexts, which can be explained by known criminological theories, has been explored and investigated. This line of investigation does not, however, examine the moderating effects of technological expertise, absorption in cyberspace, or perceptions of online anonymity. The space transition theory, as an explanation for the distinction between the causes of crimes committed online and offline. The extent to which criminals who operate in the "real world" are more inclined to participate in illegal conduct online is another issue of study in this field. Recent study has shown, for instance, that current gang members are more likely than former gang members or non-gang members to engage in online criminality. However, gang involvement in cyberspace focuses more on strengthening reputational status than increasing instrumental gains. Gang behavior in [cyberspace] focuses more on strengthening reputational standing than on generating instrumental gains. Cyberspace gang activities relies more on reputational enhancement (Pyrooz, Decker, & Moule, 2015). The research presented in this special issue contributes to these ongoing debates and demonstrates that cybercrime research is beginning to ask more nuanced questions about the role of culture, parental socialization, and self-control, as well as how offenders use technological advances to further their deviant and criminal behavior.

## References

Beech, A. R., Elliott, I. A., Birgden, A., & Findlater, D. (2008). The Internet and child sexual offending: A criminological review. Aggression and Violent Behavior, 13, 216–228. doi:10.1016/j.avb.2008.03.007.

Beech, A. R., Elliott, I. A., Birgden, A., & Findlater, D. (2008). The Internet and child sexual offending: A criminological review. Aggression and Violent Behavior, 13, 216–228. doi:10.1016/j.avb.2008.03.007.

Deviance and Social Control Summary of Topics Deviance and Social Control Functionalism and Deviance Symbolic Interactionism and Deviance Conflict Theory and Deviance Crime and Punishment What is Deviance? (n.d.). https://www.steilacoom.k12.wa.us/cms/lib/WA01001786/Centricity/Domain/70/Ch.%207%20Deviance.pdf.

Frederick, B. J., & Perrone, D. (2014). Party N play on the Internet: Subcultural formation, Craigslist, and escaping from stigma. Deviant Behavior, 35(11), 859–884. doi:10.1080/01639625.2014.897116.

Graham, R., & Smith, S. (2019). Cybercrime and Digital Deviance. Sociology & Criminal Justice Faculty Books. https://digitalcommons.odu.edu/sociology_criminaljustice_books/28/.

Lavorgna, A. (2014). Internet-mediated drug trafficking: Towards a better understanding of new criminal dynamics. Trends in Organized Crime, 27, 250–270. doi:10.1007/s12117-014-9226-8.

Pyrooz, D. C., Decker, S. H., & Moule, R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. Justice Quarterly, 32(3), 471–499. doi:10.1080/07418825.2013.778326

Rediker, E. (2015). The incitement of terrorism on the Internet: Legal standards, enforcement, and the role of the European Union. Michigan Journal of International Law, 36(32), 321–351.

Stalans, L. J. & Finn, M. A. (2016). Consulting legal experts in the real and virtual world: Pimps' and johns' cultural schemas about strategies to avoid arrest and conviction. Deviant Behavior, 37(6), 644–664. doi:10.1080/01639625.2015.1060810.

Stonard, K. E., Bowen, E., Lawrence, T. R., & Price, S. A. (2014). The relevance of technology to the nature, prevalence and impact of adolescent dating violence and abuse: A research synthesis. Aggression and Violent Behavior, 19, 390–417. doi:10.1016/j.avb.2014.06.005.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Malden, MA: Polity Press.