4.8 8 Knowledge Area: Societal Security

The Societal Security knowledge area focuses on aspects of cybersecurity that broadly impact society as a whole for better or for worse. Cybercrime, law, ethics, policy, privacy and their relation to each other are the key concepts of this knowledge area. The threat of cybercrime across the global society is incredibly serious and growing. Laws, ethics and policies are vital to the security of corporate and government secrets and assets, as well as to the protection of individual privacy and identity.

4.8.1 Knowledge Units and Topics

The following table lists the essentials, knowledge units, and topics of the Societal Security knowledge area.

SOCIETAL SECURITY		
Essentials Cybercrime, Cyber law, Cyber ethics, Cyber policy, and Privacy.		
Knowledge Units	**Topic**	**Description/Curricular Guidance**
Cybercrime		This knowledge unit aims to provide students with an understanding of the scope, cost and legal environment relating to cyber-based intellectual property theft. This includes both national and international environments. Students should have a strong understanding of the basic property-rights legislation and be able to help others navigate the complex legal and ethical world of intellectual property
	Cybercriminal behavior	Behavior that attacks individual / companies compute device or computer infrastructure to perform malicious activities, such as spreading viruses, data theft, and identity theft.
	Cyber terrorism	Activities in cyberspace geared to generate societal fear and uncertainty.
	Cybercriminal investigations	Methods for investigating cyberattacks by criminals, cybercriminal organizations, overseas adversaries, and terrorists.
	Economics of cybercrime	Risks of cybercrime are too low, while the rewards are too high, and The use of (untraceable) cryptocurrencies in committing cybercrimes online and in the Dark Web (bitcoin).

Cyber Law [*See also Organizational Security KA for related content*]		This knowledge unit aims to provide students with a broad understanding of the current legal environment in relation to cyberspace. This includes both domestic and international laws as well as the application of jurisdictional boundaries in cyber-based legal cases. Students should have a strong understanding of current applicable legislation and a strong background in the formation of these legal tools.
	Constitutional foundations of cyber law	This topic included: - Executive power, - Legislative power, - First amendment, - Fourth amendment, and - Tenth amendment.
	Intellectual property related to cybersecurity	This topic covers: - The scope, cost and legal environment relating to cyberbased intellectual property theft, - The specific content will be driven by the country of focus. In the U.S., cover Section 1201 of the Digital Millennium Copyright Act, and - Anti–circumvention - Digital Millennium Copyright Act (DMCA 1201).
[*See also Data Security KA*, *Human Security KA*, *and Organizational Security KA for related content*.]	Privacy laws	This topic includes: - Laws governing Internet privacy, - Laws governing social media privacy, and - Electronic surveillance laws, such as Wiretap Act, Stored Communications Act, and Pen Register Act.
	Data security law	This topic includes: - Section 5 of the U.S. Federal Trade Commission, - State data security laws, - State data-breach notification laws, - Health Insurance Portability Accountability Act (HIPAA), - Gramm Leach Bliley Act (GLBA), and - Information sharing through US-CERT, Cybersecurity Act of 2015.
	Computer hacking laws	This topic covers: - U.S. Federal computer crime laws, such as Computer Fraud and Abuse Act. Most computer hacking offenses are prosecuted under the Computer Fraud and Abuse Act in the U.S. - International framework and cooperation needed to prosecute overseas hackers.
	Digital evidence	This topic includes: - Forensically-sound collection of digital evidence, and - Preserving the chain of custody.

	Digital contracts	This topic includes: • Distinction among browse-wrap, click-wrap, and shrink-wrap agreements. • The Electronic Signatures in Global and International Commerce Act (ESGICA) of 2000; digital contracts and electronic signatures are just as legal and enforceable as traditional paper contracts signed in ink.
	Multinational conventions (accords)	This topic covers jurisdictional limitations of multinational accords. Examples: Budapest Convention on cybercrime and the G-7 Cybersecurity Accord on financial institutions.
[*See also Data Security KA*, *Human Security KA*, *and Organizational Security KA*, *for related content*.]	Cross-border privacy and data security laws	Requirements of the General Data Protection Regulation (GDPR). Privacy Shield agreement between countries, such as the United States and the United Kingdom, allowing the transfer of personal data.
Cyber Ethics [*See also Organizational Security KA*, *and Software Security KA*, *for related content*.]		This knowledge unit aims to give students a foundation for both understanding and applying moral reasoning models to addressing current and emerging ethical dilemmas on an individual and group (professional) level. It also sensitizes students to debates about whether ethics in computing is a unique problem or part of a larger phenomenon, and helps students to think through how their nation's culture and legal framework impact their understanding and implementation of ethics in their society.
	Defining ethics	For this topic: • Compare and contrast major ethical stances, including virtue ethics, utilitarian ethics and deontological ethics. • Apply the three different ethical stances in thinking through the ethical consequences of a particular problem or action.
	Professional ethics and codes of conduct	This topic covers: • Major professional societies, such as ACM, IEEE-CS, AIS, and (ISC)2, • Professional responsibility, and • Ethical responsibility in relation to
	Ethics and equity/diversity	For this topic: • Describe the ways in which decision-making algorithms may over-represent or underrepresent majority and minority groups in society, and • Analyze the ways in which algorithms may implicitly include social, gender and class

	Ethics and law	For this topic: • Understand that ethical practices and legal codes may not always align exactly, • Distinguish among nuisance hacking, activist hacking, criminal hacking, and acts of war.
	Ethical frameworks and normative theories	Common ethical frameworks and normative theories related to cybersecurity from individual and societal perspectives.
Cyber Policy [*See also Organizational Security KA for related content*]		The Cyber Policy knowledge unit is intended to help students understand and analyze cyber issues as they relate to the national interest generally, and to national (and national security) policy more specifically. Students are expected to gain an understanding of questions relating to the use of cyber as an instrument of war, and to distinguish between the uses of cyber as such an instrument and the possibility of cyberwar itself occurring. Students will be given an opportunity to grapple with questions regarding how the use of cyber can be signaled to other countries, as well as the challenges associated with its deterrence. Students are also expected to grasp the historical trends that have made cyber important to national policy and the development of a national cyber policy architecture. Students will be expected to demonstrate original thinking about how cyber affects the national interest, including economic, and the policy implications for national policy arising from cyber.
	International cyber policy	This topic includes: • International cyber policy challenges, • International Cyber Policy Oversight Act of 2015, and • Department of State international cyberspace policy strategy.
	U.S. federal cyber policy	This topic includes: • Federal Information Security Modernization Act, an update to the Federal Government's cybersecurity policies and guidance; • Relationship to the nation’s critical infrastructure; and • Managing risk at a national level.

	Global impact	This topic covers: • Effects of cybersecurity on the international system generally and on international security specifically. • How cyber has become and will continue to become an instrument of power, and how this power might change the balance of power between stronger and weaker countries. • Global governance of cyber. Also examine the possibilities of the development of normative behavior related to the use of cyber. • Effects of cyber on the global economy.
	Cybersecurity policy and national security	This topic covers: • How a country defines its cybersecurity policy, doctrine and execution responsibility, including national cybersecurity policy, architecture, signals and narratives, and coercion and brandishing; and • A nation's cybersecurity messaging; how it signals its intentions to gain other nation's attention and cooperation.
	National economic implications of cybersecurity	This topic covers: • The cost of cybersecurity to a nation, • The losses and gains of cybersecurity to a nation, and • The investment to keep a nation protected from cyberthreats and cyberattacks.
	New adjacencies to diplomacy	This topic covers: • The "delicate dance" of cyber diplomacy, and • Aspects of cybersecurity that have become part of the relationships between countries, including the covert collection of information alongside the practice of diplomacy, and the covert application of cyberforce in cyberspace and physical space.
Privacy [*See also Human Security KA*, *Organizational Security KA*, *and Data Security KA*, *for related content.*]		This knowledge unit is intended to provide students with an understanding of privacy and its related challenges. Students are expected to understand the tradeoffs of sharing and protecting sensitive information; and how domestic and international privacy rights impact a company's responsibility for collecting, storing and handling personal data. Students will gain an understanding of privacy-enhancing technologies and security application, which can include the concepts of appropriate use, as well as protection of information.

	Defining privacy	For this topic: • Apply operational definitions of privacy, • Identify different privacy goals, e.g., confidentiality of communications and privacy of metadata, and • Identifying privacy tradeoffs – increasing privacy can have risks (e.g., the use of Tor could make someone a target for increased government scrutiny in some parts of the world).
	Privacy rights	For this topic: • Describe informed consent conditions in relation to personal data collection and sharing, • Recognize national privacy rights in the existence of privacy rights, and • Demonstrate familiarity with the debate about
	Safeguarding privacy	For this topic: • List cyber-hygiene steps to safeguard personal privacy, • List privacy-enhancing technologies and their use and the properties that they do and do not provide (i.e., Tor, encryption), • Describe conditions for ethical and lawful use of privacy enhancing technologies • Describe steps in carrying out a privacy impact assessment, • Describe the role of the data trustee, • Describe legislation related to data localization practices, • Demonstrate an understanding difference between privacy rights and privacy-enhancing capability – operationalizing privacy, and • Discuss the dynamic impact of metadata and big data on privacy.
	Privacy norms and attitudes	This topic includes: • Privacy calculus theory and models, and • Cultural differences in the existence of privacy norms and boundaries.
	Privacy breaches	This topic covers the role of corporations in protecting data and addressing circumstances when data privacy is compromised.
	Privacy in societies	This topic includes: • Privacy rights and threats to privacy related to public figures, • Differential surveillance and its risks; challenges for smart cities, and • Harm matrix for cybersecurity surveillance.

4.8.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	**Learning outcomes**
Cybercrime	
	Discuss various motives for cybercrime behavior.
	Summarize terror activities in cyberspace geared toward generating societal fear and certainty.
	Describe methods for investigating both domestic and international crimes.
	Explain why preserving the chain of digital evidence is necessary in prosecuting cybercrimes.
Cyber law	
	Describe the constitutional foundations of cyber law.
	Describe international data security and computer hacking laws.
	Interpret intellectual property laws related to security.
	Summarize laws governing online privacy.
Cyber ethics	
	Distinguish among virtue ethics, utilitarian ethics and deontological ethics.
	Paraphrase professional ethics and codes of conduct from prominent professional societies, such as ACM, IEEE-CS, AIS and $(ISC)^2$.
	Describe ways in which decision-making algorithms could over-represent or under-represent majority and minority groups in society.
Cyber policy	
	Describe major international public policy positions and the impact they have on organizations and individuals.
	Summarize nation-specific cybersecurity public policy with respect to the protection of sensitive information and protection of critical infrastructure.
	Explain global impact of cybersecurity to culture including areas such as the economy, social issues, policy and laws.
Privacy	
	Describe the concept of privacy including the societal definition of what constitutes personally private information and the tradeoffs between individual privacy and security.
	Summarize the tradeoff between the rights to privacy by the individual versus the needs of society.
	Describe the common practices and technologies used to safeguard personal privacy.