CCDC DAC-TR-2020-003
January 2020

Cyber and Electromagnetic Activities (CEMA) Operations Impacts on Human Performance Final Report

by Christopher Plott and John Keller

DISCLAIMER

The findings in this report are not to be construed as an official Department of the Army position unless so specified by other official documentation.

WARNING

Information and data contained in this document are based on the input available at the time of preparation.

TRADE NAMES

The use of trade names in this report does not constitute an official endorsement or approval of the use of such commercial hardware or software. The report may not be cited for purposes of advertisement.

CCDC DAC-TR-2020-003
January 2020

Cyber and Electromagnetic Activities (CEMA) Operations Impacts on Human Performance Final Report

by Christopher Plott and John Keller
Alion Science and Technology

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED *(From - To)*
January 2020	Contractor Report	9/30/2018 – 9/30/2019

4. TITLE AND SUBTITLE
Cyber and Electromagnetic Activities (CEMA) Operations Impacts on Human Performance Final Report

5a. CONTRACT NUMBER
W911QX-18-C-0050

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Christopher Plott and John Keller

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Alion Science and Technology
246 S Taylor Ave, Suite 300
Louisville, CO 80027

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army CCDC Data & Analysis Center
6896 Mauchly Street
Aberdeen Proving Ground, MD

10. SPONSOR/MONITOR'S ACRONYM(S)
CCDC DAC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
CCDC DAC-TR-2020-003

12. DISTRIBUTION / AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In this report we review the cyber and electromagnetic activities (CEMA) threats and attacks that can impact human performance. We then use the available data to translate these impacts, as best we can, into algorithms that can be used in human performance models. Since many of the threats, attacks, and impacts are dependent on the context of their use and what or who is targeted, we provide a framework for the development of scenarios for building and exercising human performance models that incorporate the CEMA threats, attacks, and impacts, with a focus on cyber defense operations and the cyber defense analyst.

15. SUBJECT TERMS
CEMA attacks, cyber security, human performance, stress and decision making, cyber defense analyst, cyber threat scenarios

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	SAME AS REPORT	59	Christopher Garneau
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			19b. TELEPHONE NUMBER *(include area code)* (410) 278-5814

Table of Contents

List of Figures

List of Tables

1. INTRODUCTION

The Army and their opponents use cyber and electromagnetic activities (CEMA) for conducting cyberspace and electronic warfare operations. Army Field Manual No. 3-12: Cyberspace and Electronic Warfare Operations (Department of the Army, 2017) describes the threats in cyberspace as follows:

> The Army faces multiple, simultaneous, and continuous threats in cyberspace. A threat is any combination of actors, entities, or forces that have the capability and intent to harm the United States forces, United States national interests, or the homeland. Threats include state and non-state actors, criminals, insider threats, and the unwitting individuals who intend no malice. These diverse threats have disparate agendas, alliances, and range of capabilities. Enemies and adversaries employ regular and irregular forces and use an ever-changing variety of conventional and unconventional tactics. Risks from insiders may be malicious or cause damage unintentionally. Insider risks include non-compliance of policies and regulations, causing vulnerabilities on the network.

The electromagnetic spectrum and wired computer and communications networks are both essential infrastructure to be protected as well as the means for CEMA attacks. Various parts of the electromagnetic spectrum at sufficient energy levels can be used to disrupt, disable, or take over these networks and their associated equipment and systems.

The Army must be able to defend and respond to this wide range of threats and attacks. Many types of CEMA attacks affect either hardware or software technology and cause direct or indirect damage to these technologies or to the technologies, systems, or operations they support. Other types of threats and attacks focus on the humans using or supporting the hardware, software, and associated systems and operations. These attacks use social engineering or deception, and take advantage of poor security behavior and poor decision making on the part of the targeted people. A more limited set of threats and attacks can cause actual physical harm to, or temporarily disable, the targeted personnel.

In this report we review the CEMA threats and attacks that can impact human performance. We then use the available data to translate these impacts, as best we can, into methods or algorithms that can be used in human performance models. Since many of the threats, attacks, and impacts are dependent on the context of their use and what or who is targeted, we provide a framework for the development of scenarios for building and exercising human performance models that incorporate the CEMA threats, attacks, and impacts, with a focus on cyber defense operations and the cyber defense analyst.

2. THE CHARACTER OF CEMA THREATS AND ATTACKS

CEMA threats can include a wide range of actors who have a diverse set of goals. The attacks can produce immediate or delayed impacts, or may be more clandestine and difficult to discover. The means of attack can include hardwired computer networks or any part of the electromagnetic spectrum used for digital or analog electrical communication. Parts of the electromagnetic spectrum can also be used to cause direct physical harm or disruption to both equipment and people. In this section we characterize the range of CEMA threats and attacks that can impact human performance.

The Intel Information Technology Threat Assessment Group (Casey, 2007) has developed a Threat Agent Library that systematically identifies a wide range of both hostile and nonhostile threat types as well as their means and intent for attack. They identify over 150 combinations of means and intent that can be used by threat agents. Sanger (2017) itemizes the following advantageous and disadvantageous uses of cyber capabilities:

Advantageous

- Cyber strikes can be dialed up and dialed back, theoretically making it easier to control damage inflected.
- Most cyber strikes do not necessarily lead to fatalities.
- If the strike is well hidden from the target, the target can be hit repeatedly and the size of the attacks can be controlled.
- Responsibility for cyber strikes is often plausibly deniable and can possibly be redirected to another actor (i.e., difficulty in attribution).
- No geographic limitations.

Disadvantageous

- Results can be significantly more unpredictable than advocates admit.
- Immediate impact can be difficult to assess depending on the inner workings of the target and the intelligence about the target.
- Long-term consequences are almost impossible to anticipate.
- Due to attacker attribution and intent difficulties, preemptive strikes can be risky and difficult to justify.

Gavin (2017) provides these further considerations when using cyber attacks:

- It is difficult to identify the sources of a cyber event and even more so to measure the cyber capabilities before they have been used.
- Cyber capabilities may increase the speed of a conflict once started.

- By compressing the time available to make decisions, cyber can overwhelm institutions, organizations and individuals who are used to a more deliberate battlefield.
- Cyber capabilities are neither static nor linear; they can adapt as battle goes on and, in conjunction with other military capabilities, may have multiplier effects in conflict.
- Cyber attacks may be oriented in comprehensive ways at the participant's command, control, communications, and intelligence capabilities, blinding either one or all sides to what is happening on the battlefield.
- These qualities may increase the incentive to use cyber preemptively, as there may be large first-mover advantages.
- These characteristics may also impede war termination or efforts to prevent escalation, as one side or another may lose the capability to assess the battlefield and might assume the worst.

These insights reflect the dynamic and uncertain decision environment that cyber defenders must work in and that the consequences of poor decisions or inappropriate action (or inaction) can be high.

CEMA attacks can be broadly divided into attacks using software working through computer hardwired and wireless networks, commonly referred to as cyber attacks, and attacks using the parts of the electromagnetic spectrum to create physical effects. In this section we discuss the specific types of attacks that have been made using CEMA. Since the character of physical and cyber attacks are very different, we discuss their impacts on human performance separately.

A useful framework for characterizing and addressing CEMA attacks is the Cyber Kill Chain originally developed by Lockheed Martin Corporation (2015), which describes the phases of a cyber attack. According to Lockheed Martin, threats must progress through several steps in the model in order. These steps are as follows:

1. Reconnaissance: Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.
2. Weaponization: Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.
3. Delivery: Intruder transmits weapon to target (e.g., via e-mail attachments, websites, or USB drives).
4. Exploitation: Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.
5. Installation: Malware weapon installs access point (e.g., "backdoor") usable by intruder.
6. Command and Control: Malware enables intruder to have "hands on the keyboard" persistent access to target network.
7. Actions on Objective: Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.

Melnick (2018) itemized the most common types of cyber attacks, which at a high level include

- Denial-of-service (DoS)
- Distributed denial-of-service (DDoS)
- Man-in-the-middle (MitM) attack
- Phishing attack
- Spear phishing attack
- Drive-by attack
- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack

Appendix B provides full descriptions and different variations for each of these types of cyber attacks.

Lindberg et al. (2018) have extended the Cyber Kill Chain concept, with supplements from Department of the Army (2017), to include electromagnetic effects as well as, which include

- Radio frequency identification
- Radio frequency direction finding
- Electromagnetic jamming
- Electro-optical-infrared jamming
- Radio frequency jamming
- Electromagnetic pulse
- Electronic probing
- Obtaining stolen certificates
- Exploiting unencrypted messages
- MitM attack
- Message spoofing
- GPS spoofing
- Electromagnetic deception
- Electromagnetic intrusion
- Beaconing using the electromagnetic spectrum

Appendix C provides full descriptions for each of these types of electromagnetic attacks.

In addition to the electromagnetic effects described in the Appendix C table, many nonlethal weapons are using the various parts of electromagnetic spectrum for their effects. This can

include technologies such as dazzlers, stun grenades, lasers, and tasers. These effects and the use of an electromagnetic pulse are the only attacks of those listed that cause direct physical harm. The electromagnetic attacks and cyber attacks are otherwise fairly similar except that the electromagnetic attacks use the electromagnetic spectrum as the means for accessing that targeted network or equipment.

3. CEMA HARMS AND EFFECTS ON HUMAN PERFORMANCE

In this section we address the various kinds of impacts of CEMA attacks on human performance and how the effects might be incorporated into human performance models of cyber defender operations. At the most basic level, the attacks can impact the tasks that are performed by cyber defenders. Many of these attacks are deceptive, difficult to detect, and may lay dormant. As a result, CEMA defenders may end up performing inappropriate tasks that can enable the attacks, have current tasks disrupted, and may initially perform incorrect tasks if they misinterpret what is happening in the attack. These kinds of effects can be incorporated into human performance models by elaborating on baseline task performance models to include a greater range of, or more detailed understanding of, attack detection, response and recovery tasks, task flows, and sequencing logics, as well as inclusion of erroneous response tasks and probabilities of their occurrence.

Agrafiotis et al. (2018) provide a taxonomy of cyber-harms. The primary cyber-harm types include physical or digital, economic, psychological, reputational, and social/societal. For the purposes of this review, the physical and psychological harms are of greatest interest. The subtypes of harm for the physical or digital harm type include the following:

- Damaged or unavailable: The asset has been physically or digitally affected to the point where it is not available to fulfil its intended purpose.
- Destroyed: The asset has been physically or digitally ruined.
- Theft: The asset has been physically or digitally stolen.
- Compromised: The asset has been physically or digitally affected.
- Infected: The asset has been physically or digitally contaminated.
- Exposed or leaked: The asset has been physically or digitally disclosed.
- Corrupted: The asset has been physically or digitally debased or its integrity affected.
- Reduced performance: The asset has had its ability to function lowered.
- Bodily injury: The body of the human asset has been wounded.
- Pain: The human asset has experienced agony.
- Loss of life: The human asset is no longer alive.
- Prosecution: Legal proceedings have been launched against an individual or organization.
- Abuse: The asset has been physically or digitally misused.
- Mistreatment: The asset has been physically or digitally brutalized.
- Identity theft: The theft of personal identity information.

The outcomes of these harms can be categorized into physical harm to the targeted individual(s), harm to equipment or information, and potential for secondary psychological, reputational, or social/societal harm. We address physical harm to the targeted individual(s) in the next subsection on electromagnetic effects on human performance. Harm to equipment or

information results in changes to the tasks and actions the targets can take to further their goals or mitigate the effects of the attack. The secondary psychological harms have the potential to result in any of the subtypes of the psychological harm type, which include

- Confusion: Disarray experienced by the organization's stakeholders.
- Discomfort: Uneasiness experienced by the organization's stakeholders.
- Frustration: Dissatisfaction experienced by the organization's stakeholders.
- Worry or anxiety: Nervousness experienced by the organization's stakeholders.
- Feeling upset: Anger experienced by the organization's stakeholders.
- Depressed: Low-spiritedness experienced by the organization's stakeholders.
- Embarrassed: Humiliation experienced by the organization's stakeholders.
- Shameful: Disgracefulness experienced by the organization's stakeholders.
- Guilty: Regret or remorsefulness experienced by the organization's stakeholders.
- Loss of self-confidence: Lack of courage or certainty experienced by the organization's stakeholders.
- Low satisfaction: Lack of contentment experienced by the organization's stakeholders.
- Negative changes in perception: An adverse change in how stakeholders regard a stakeholder.

Duggan (2017) further elaborates on cognitive attacks that "… can exploit human blind spots, biases, decision-making heuristics, preferences, target the way adversaries assign meaning to content, exploit human machine interfaces, take covert or overt approaches, use misinformation, manipulate information, present unreal problems, and on and on". Specifically, he identifies the cognitive strategies of preclusion, attacking will, and cultural stand-off:

- *Preclusion* focuses on psychologically containing an adversary in the hopelessness, isolation, and futility of his plight.
- *Defeating Enemy-Will* is specifically designed to undermine and destroy the adversary's will to fight. Attacking enemy-will values psychological impact above all else, and employs CEMA to inflict highly visible embarrassing losses, whether fabricated or real, shame the enemy, pit elements of an adversary against one another, and a host of other methods.
- *Cultural Standoff* specifically focuses CEMA on better understanding the context of people's lives and cultures and then using that knowledge to transform indirect influence into coercive means.

These psychological harms can disrupt the ability of the targeted people to perform their tasks or pursue their intended goals due to psychological stress that can interfere with decision making and task performance, and in extreme cases result in emotional trauma.

In the following subsections we first discuss the physical impacts of CEMA attacks on human performance. Since many CEMA attacks are based on various forms of deception, we discuss their psychological impacts on decision making, and in particular on the influence of decision-making biases that attackers may try to take advantage of. Finally, since CEMA attacks can also be targeted at demoralizing targeted people, we look at the impacts of stress on decision making and people's ability to respond to the attack.

3.1 CEMA Physical and Physiological Effects on Human Performance

Determining the effects on human performance of exposure to radiating energy across the electromagnetic spectrum depends on the electromagnetic sources, energy levels, and biological effects of the exposure. While not normally included in discussions of CEMA, we also address the effects of nonlethal weapons that use the part of electromagnetic spectrum to produce their effect. This information was then evaluated for potential use in human performance modeling.

As illustrated in Figure 1 (Department of the Army, 2017), the spectrum range of interest includes ultraviolet, visible light, infrared, microwave, radio, and sonic. We do not include the ionizing radiations of X-ray or gamma ray; however, electromagnetic pulses resulting from these types of events can totally disable electronic equipment. While not generally considered part of the electromagnetic spectrum, sonic effects were included based on their similarity as a propagating wave form and their use in directed energy weapons to affect human performance. Lasers, covering the frequency range from ultraviolet to infrared, are treated as a separate category due to the unique effects of highly focused energy beams.

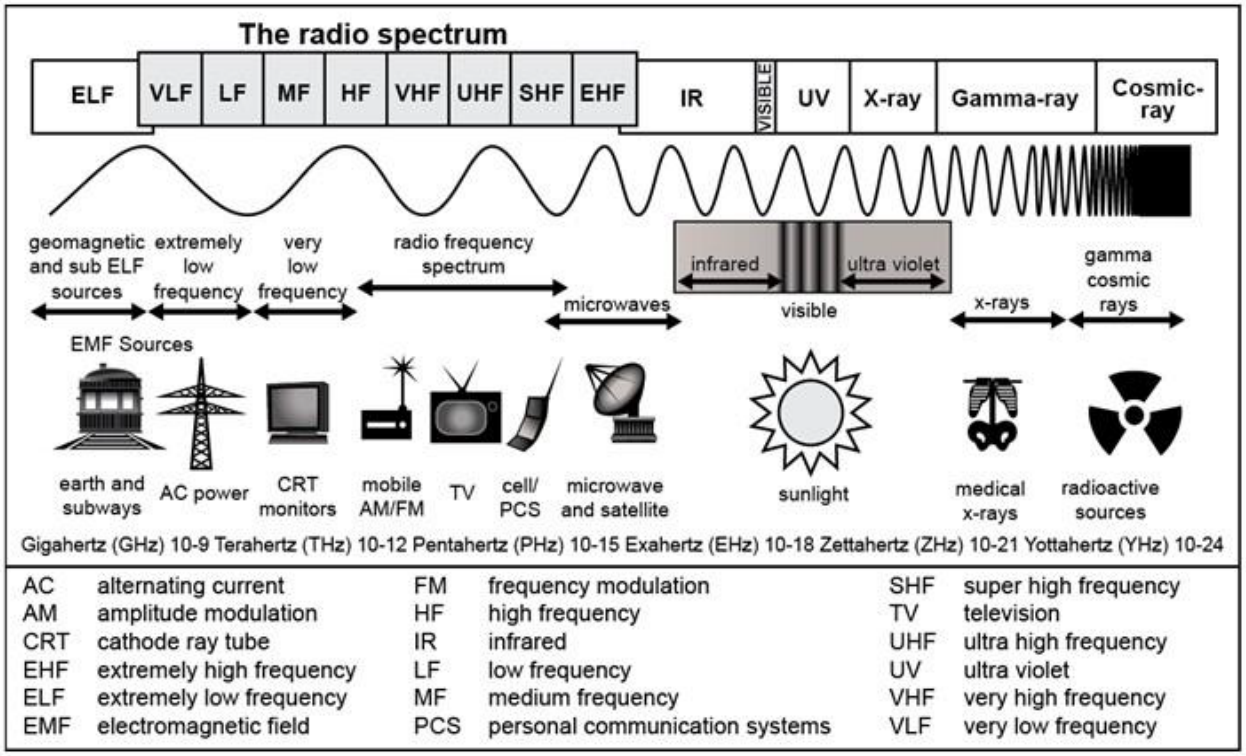

Figure 1. Electromagnetic spectrum with example sources and uses

Long-term exposures are not addressed as part of this review. There are many well-researched effects to human health from cumulative exposures across the energy spectrum. However, human performance modeling focuses on periods from seconds to hours. As such, this review has focused on energy effects and systems that are shown to affect human performance in the short term.

Effects across the spectrum are a function of the field type, energy level, exposure duration, and anatomy component. The most common effect is some level of heating to either surface or internal tissues. The human eye is especially vulnerable across the spectrum but is at highest risk from nonvisible radiations. The effects to performance range from low levels of irritation to incapacitation and death. At higher energy levels, the effects can be similar to being shot in that the duration is extremely fast and the level of incapacitation depends on the portion of the anatomy affected. The nonlethal systems attempt to deter or temporarily incapacitate and can have effects lasting up to several minutes. Table 1 provides a summary of the spectrum, example weapons systems, and associated effects.

Table 1. Electromagnetic Spectrum Ranges with Biological Effects, Example Weapons Systems, and Human Performance Effects

Spectrum	Frequency	Biological Effect	Weapon System Example	Performance Effects
Ultraviolet	30 PHz–750 THz	Erythema (sunburn)	None identified	Short-term irritation Ocular pain, blurred vision
Visible Light	770 THz–400 THz	Thermal and photochemical to eyes	LED Incapacitator Dazzler Stun grenade	Temp loss of vision
Infrared	400 THz–300 GHz	Thermal to skin	None Identified	Irritation, pain, and incapacitation
Laser	30 PHz–300 GHz	Thermal and photochemical to skin and eyes	Dazzler High-energy Laser (HEL) systems	Temporary visual incapacitation Serious ocular damage Burns
Microwave	300 GHz–300 MHz	Thermal to skin and internal tissues Auditory effect	Millimeter wave (ADS)	Evade response Burns
Radio	300 MHz–3 KHz	Burns Electrical stimulation	Taser	Irritation, pain, and incapacitation
Sonic	10 KHz–20 Hz	Auditory effects Organ damage	Long-range acoustic deterrence Stun grenade	Temporary disorientation Serious injury

A detailed review is included in Appendix D. The spectrum is broken down by common identifiers and their associated frequency ranges. Each spectrum range includes a list of example sources, uses, biological and human performance effects, example weapon system(s) when available, and a discussion of the application to human performance modeling.

Most of the effects to performance are simple task interruptions. The duration of the interruption or ability to restart or continue a task will vary with the situation. While not lethal, any disabling effect occurring while operating a vehicle, for example, could have resulting injury effects.

3.2 CEMA Psychological Effects on Human Performance

When addressing psychological CEMA effects, it is useful to think about them in terms of those that occur pre-attack-event and those that occur post-attack-event. For our purposes we are

defining an attack-event as the recognition by the CEMA defender that an attack is occurring or has already occurred. In a pre-attack event, the attacker is acting somewhere in the cyber-kill chain and is trying to do one or more of the following:

- Avoid detection
- Probe for either technical or human weaknesses
- Deliver or install the attack
- Activate and use the attack without detection
- Activate and sustain the attack with detection

In these circumstances, the attacker is trying to deceive or misdirect the CEMA defender, or even promote desired defender actions. A key area of human vulnerability in this phase is defender decision making and decision-making biases that can be exploited.

Post-attack-detection is when the attacker is trying to fully execute and perhaps sustain the attack. The CEMA defender is now working to take action to end or mitigate the attack and is experiencing and responding to the outcomes of the attack. The same decision-making considerations as pre-attack-detection are in play, but they are now subject to the emotional responses of the defender. These responses may include any number of those identified previously by Agrafiotis et al. (2018) and Duggan (2017), but from the perspective of the impact on human performance, these emotions are experienced as stress. This stress can exacerbate the impacts on decision making. Based on this, we further examine decision-making biases and the impact of stress on decision making.

3.2.1 Decision-Making Biases

Issitt (2018) itemizes the following biases in reasoning and decision making that humans are prone to suffer from:

- Confirmation Bias: People are more willing to accept information that confirms what they already feel or believe.
- Proportionality Bias: People are more likely to believe statements or ideas proportional to how impactful or important they see certain issues (e.g., the belief that the magnitude of an event needs an explanation of similar magnitude, which can lead to conspiracy theories).
- Projection: People tend to project their motivations or emotions onto others (e.g., the expectation that your feelings about me are the same as mine about you).
- Desire to be Unique: An individual's desire to be unique leads them to gravitate away from mainstream consensus toward behaviors, beliefs, and groups that they see as more unique or unusual.

- Generalization: Believing that an individual's specific experience generalizes to broader contexts.
- Post Hoc Ergo Propter Hoc: Assuming causal connections between things without evidence.
- Motivated Reasoning: A person is thinking about an issue and is "motivated" to find an answer, usually quickly, so fall subject to the previous biases.

Kahneman (2011) identifies the additional biases relevant to CEMA-related decision making shown in Table 2.

Table 2. Decision-Making Biases

Bias	Description
Priming Effects	Exposure to an idea "primes" the mind to associate related ideas and actions both consciously and subconsciously.
Framing Effects	Different ways of presenting the same information often evoke different emotions and judgements. Unless there is an obvious reason to do otherwise, most people passively accept decision problems as they are framed and therefore rarely have an opportunity to discover the extent to which their preferences are frame-bound rather than reality-bound.
Frequency Bias	Frequent repetition of information, true or false, produces familiarity. Familiarity is often not easily distinguishable from truth.
Representativeness Bias	People have norms or prototypical examples for a vast number of categories. Stereotypes, both correct and false, are how people think of categories. People will rely on stereotypes, or representativeness, rather than base rate or reliability information when making estimates of probability or likelihood, and they tend to be insensitive to the quality of evidence.
Hindsight Bias	People tend to assess the quality of a decision not by whether the process was sound but whether the outcome was good or bad.
Law of Large Numbers Bias	People have strong bias toward believing that small samples closely resemble the population from which they are drawn and behave as if the Law of Large Numbers (Large samples are more precise than small samples) applies to small numbers as well. People are too willing to reject the belief that much of what they see in life is random.
Affect Heuristic	People let their likes and dislikes determine their beliefs about the world. This includes the "Halo Effect" which is the tendency to like (or dislike) everything about a person, thing or situation – including things not observed.
Overconfidence	The confidence that individuals have in their beliefs depends mostly on the quality of the story they can tell about what they see, even if they see little. People often fail to allow for the possibility that evidence that should be critical to their judgement is missing. People tend to settle on a coherent explanation and suppress doubt and ambiguity.

Table 2. Decision-Making Biases

Bias	Description
Risk Aversion and Risk Taking Biases	• People are averse to risk when they consider prospects with a substantial chance to achieve a large gain. They are willing to accept less than the expected value of a gamble to lock in a sure gain. • When the chance of a gain is large, people are indifferent to the fact that the chance of winning is miniscule. They are willing to pay more than the expected value of a gamble for a chance at a large gain. • People are willing to pay more for protection against an unwanted loss than the expected value of the loss (insurance). • People are more willing to take a gamble on a larger loss (hope) than to accept a sure loss. • People overestimate the probabilities of unlikely events. • People overweight unlikely events in their decisions.

Kahneman (2011) also identifies a number of mechanisms for mitigating decision-making biases, including the following:

- Learning to recognize situations in which mistakes are likely and try harder to avoid significant mistakes when stakes are high.
- Seek multiple sources of evidence that are independent of each other.
- Work to apply disciplined Bayesian reasoning, which can be simply summarized as
    - Anchoring judgement of the probability of an outcome on a plausible base rate.
    - Question the diagnosticity of the evidence.
- Use standard polices, operating procedures, and simple checklists whenever possible.

To be useful in human performance modeling, these biases need to be put in the context of the type of decision that is being made, the information that is available, the susceptibility of the defender to the bias, and the general context in which the decision is being made. While decisions that are made frequently might be generalizable across models or within a model, most of the time each decision task will need to be examined in context to determine which decision biases apply, their likelihood of occurring, and the consequences to the task.

In terms of likelihood, unless there has been training to avoid the bias, good cognitive discipline is expected, or other protective mechanisms are in place (e.g., default action), the literature suggests that most of these biases are likely to occur. While few actual base rate estimates are given, a 50-50 likelihood does not seem unreasonable.

With regard to consequences, these are typically reflected in human performance models by changes in task times or alternate decisions that result in different task actions from the baseline or desired task flow.

3.2.2 Stress and Decision Making

The decision-making biases discussed previously can be exacerbated and new decision-making degradations can be introduced when decision makers experience stress. As defined by Marin et al. (2010), stress is

> a threat, real or implied, to the physical (i.e., homeostasis) or psychological integrity of an individual. In this sense, stress can be absolute (a real threat induced by an earthquake for instance, leading to a significant stress response in every person facing this threat), or it can be relative (an implied threat induced by the interpretation of a situation as being novel and/or unpredictable and/or uncontrollable and/or threatening for the ego; e.g., a public speaking task).

Both improved performance and performance degradation have been associated with increased stress (Kowalski & Vaught 2003; LeBlanc 2009). Stress is affected by perception: stressful circumstances do not automatically lead to problems in judgement; it is the perceived experience of distress that can affect judgment (Gillis 1993; Kowalski & Vaught 2003). LeBlanc further explains that the experience of stress is heavily influenced by the person's assessment of the situation:

- When individuals perceive a real or anticipated challenge to their primary goals, they appraise the situation in a two stage process: 1) They assess the demands of the situation, and then 2) they assess the resources available to meet the perceived demands of the situation.
- When the resources are assessed as sufficient, the situation is assessed as a challenge and a positive psychological state of eustress ensues.
- When demands are assessed as exceeding resources, the situation is assessed as a threat and a negative psychological state of distress ensues.

Any factor that increases demands or decreases resources, increases the likelihood of distress. These perceptions can be moderated by training and experience. People with more experience and training tend to report less stress (Kowalski & Vaught, 2003). They use their experience to identify meaningful data and generate reasonable options, and they use simplifying heuristics to select a course of action and then implement the first workable solution (Gok & Atsan, 2016).

In addition, significant individual differences in stress responses and performance are influenced by the following (LeBlanc, 2009):

- *Coping Styles. Problem-focused coping* consists of addressing the problem causing the distress. *Emotion-focused coping* is aimed at reducing and managing the emotional distress associated with the situation. *Avoidance coping* is aimed at seeking to avoid or distract oneself from the situation.

- *Control.* The extent to which an individual perceives that they have control over a given situation. People with an *internal locus of control* perceive a feeling of being able to control events and are likely to develop a positive outcome expectancy; consequently, they have lessened stress responses and performance impairments under acute stress.
- *Social Support.* Individuals who have access to psychological support in demanding situations experience less stress.

Given these considerations, and the nature of the cyber workforce (highly trained, highly skilled, resilient, social/organizational support, etc.), we can expect stress to impact their decision making to some degree, but it will likely be moderated relative to the general population.

According to Kowalski & Vaught (2003), and reinforced by LeBlanc (2009) and Gok & Atsan (2016), specific ways that stress has been shown to influence decision making and performance include the following:

- If a situation involves risk, people become more cautious and adopt risk avoiding behavior with importance placed on avoiding losses.
- People adopt simpler modes of information processing in which alternatives are not fully explored and certain important cues are used to determine the decision.
- The focus of attention shrinks, and the individual focuses on just critical issues and elements.
- Stress was found to induce a tendency to offer solutions before all decision alternatives had been considered and to scan such alternatives in a non-systematic fashion.
- When information is expensive in time and actions are cheap, people still tend to choose further information over action.

LeBlanc (2009) elaborates further on stress effects on attention directing behavior as follows:

- When feeling anxious, people's attention is biased toward threat-related information.
- If the task being performed is integrally related to the source of the stress, selective attention will typically be narrowed toward the task itself.
- If the source of the stress is peripheral to the task being performed, then attention will be focused on the source of the stress, to the increasing exclusion of information related to the task itself.
- There is consistent evidence that *divided attention* tasks are vulnerable to the effects of stress, with performance being impaired under stress.

LeBlanc (2009) also elaborates on stress effects on memory as follows:

- Working memory is impaired when the individual exhibits a threat response, but not when they exhibit a challenge response.

- At moderate stress levels, memory consolidation is enhanced, especially for emotionally laden information, but is impaired at high levels of stress.
- Information from a to-be-remembered event will be retained quite well if it is that event that causes the stress response. If the stress is caused by something peripheral, consolidation is not enhanced.
- Stress leads to impairments in the retrieval of memories when there is a threat response but not when there is a challenge response.

A final consideration is the impact of extreme or traumatic stress that results in the loss of willingness to respond or "freezing." A limited laboratory study by Schmidt et al. (2008) suggests that approximately 13% of their study population experienced feelings of immobility.

Like modeling decision biases, to be useful in human performance modeling, these stress effects need to be put in the context of what type of decision is being made, what biases are already associated with the decision, the likely defender perception of the stressor, and the general context in which the decision is being made. More novel or unexpected stressors will generally increase task performance time. More highly trained defenders and the presence of protective mechanisms will mitigate the impact of stress. Otherwise, stress will result in some increase in the effects of the biases associated with the task.

4. CEMA SCENARIOS FRAMEWORK AND HUMAN PERFORMANCE MODEL DEVELOPMENT

Modeling the effects of CEMA on human performance requires a scenario or set of scenarios that cover the range of CEMA performance effects as well as realistic operational scenarios that include a robust set of cyber defender tasks. It also requires a mapping of the effects to the tasks and the impact of those effects on the tasks. We start by providing a basic description of CEMA defender operations and the role and tasks for the cyber defense analyst as our target population. We then discuss sources of scenarios, the general features desired, and the steps for developing them.

4.1 CEMA Defensive Operations and the CEMA Defender

As defined by *Field Manual No. 3-12: Cyberspace and Electronic Warfare Operations* (Department of the Army, 2017):

> *Defensive Cyberspace Operations (DCO)* are passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. DCO are threat-specific and mission prioritized to retain the ability to use the Department of Defense Information Network (DODIN). The Army uses a defense-in-depth concept, incorporating a layered approach to defend the network.
>
> The two types of DCO are Defensive Cyberspace Operations-Response Action (DCO-RA) and Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM). Both are threat-specific and defend the DODIN, but the similarity ends with that purpose. DCO-RA is more aligned with Offensive Cyberspace Operations (OCO) in execution, authorities, and techniques supporting the mission. DCO-IDM include mission assurance actions.
>
> DCO respond to unauthorized activity, alerts, and threat information against the DODIN, and leverages intelligence, counterintelligence, law enforcement, and other military capabilities as required. DCO include outmaneuvering adversaries taking or about to take offensive actions against defended networks, or responding to internal and external cyberspace threats. DCO also include actively hunting for advanced internal threats that evade routine security measures. DCO consist of those actions designed to protect friendly cyberspace from enemy and adversary actions.

For our purposes, we will focus on Warfighters who perform DCO-IDM, and specifically the cyber defense analyst. The National Institute of Science and Standards has published the *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (Newhouse et al., 2017), which

- Breaks out and organizes all of the cybersecurity related jobs
- Provides high-level descriptions for each job
- Provides detailed tasks, knowledge, skills, and abilities (KSAs) for each job

This provides a very useful resource for human factors and human performance modeling research. Within the context of a given scenario, the tasks can be organized into an initial set of baseline task flows to support model development. The KSAs can be used to provide context for job performance.

With 33 distinct jobs identified, we are focusing initially on the cyber defense analyst who has a specialty area description or work role:

> "***Specialty Area Description***: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, or networks from threats."
>
> "***Work Role***: Uses data collected from a variety of cyber defense tools (e.g., IDS [intrusion detection system] alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats."

We also focus on those tasks where the cyber defense analyst is actively engaged in real-time network/system defense as these are likely to create greater time pressure, cognitive demand, and the need for rapid decision making. Table 3 lists these tasks.

Table 3. Cyber Defense Analyst Real-Time Engagement Tasks

Task ID	Task
T0023	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.
T0155	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.
T0164	Perform cyber defense trend analysis and reporting.
T0166	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.
T0198	Provide daily summary reports of network events and activity relevant to cyber defense practices.
T0214	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.

Table 3. Cyber Defense Analyst Real-Time Engagement Tasks

Task ID	Task
T0258	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.
T0259	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.
T0260	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.
T0293	Identify and analyze anomalies in network traffic using metadata.
T0294	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).
T0295	Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.
T0296	Isolate and remove malware.
T0297	Identify applications and operating systems of a network device based on network traffic.
T0298	Reconstruct a malicious attack or activity based off network traffic.
T0299	Identify network mapping and operating system (OS) fingerprinting activities.
T0310	Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.
T0332	Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.
T0503	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
T0504	Assess and monitor cybersecurity related to system implementation and testing practices.

4.2 Development of CEMA Scenarios to Support Human Performance Modeling

This section provides a roadmap for future work in the area of developing scenarios for modeling the impacts of CEMA on cyber defender performance. We discuss several sound sources of CEMA scenarios that could be used as a starting point. We then discuss how our previous findings on physical and psychological human performance impacts can integrated into the models.

Lindberg et al. (2018) provide an initial set of short CEMA scenarios that could be implemented in training simulators. Duggan (2017) provides a robust scenario focusing on cognitive attacks. Pols (2017) provides several real-world scenarios based on both test cases used by cybersecurity

firms to challenge client cybersecurity defenses, as well as actual case studies of effective cyber intrusions. These all can be used to support the development of an overarching scenario for human performance modeling. We also believe it would be very beneficial to align with any available CEMA training scenarios that could help support model validation. Scenarios for CEMA that include effects such as those used nonlethal weapons and electromagnetic pulses might particularly benefit from human performance modeling since these types of effects would not normally be included in training.

The scenario would also need to focus on the scope of activities supported by the cyber defense analyst. The tasks and KSAs developed by Newhouse et al. (2017) provide an excellent starting point. With the addition of a realistic concept of operations and current tactics, techniques, and procedures used by Army CEMA defense operations, task flows for base models can be developed. Task time estimates would also need to be gathered.

4.3 Human Performance Model Development

With the cyber defender tasks defined, we would assess each type of CEMA attack to determine which kinds of tasks they would impact, and what the impact on the task would be. These impacts would typically include the following:

- The ability to perform the task at all
- Effects on task duration and timing
- Changes to any decision logic associated with the task
- Changes to subsequent task flows

Physical and deception effects would commonly cause direct changes in the tasks performed. Psychological and cognitive effects would affect the decision-making tasks. We would also determine what decision-making biases or stress effects could influence these tasks. Given those, we could determine how the task characteristic, including actual task execution (i.e., does it happen at all), subsequent task flows, and task durations may be affected and define additional tasks and task flows to accommodate the potential impacts of the CEMA actions and the applicable bias and stress effects.

With the base task flows and attack effects mapped onto the tasks, we would look at the CEMA actions taken against the cyber defense analyst in the scenario(s) and assess their impacts. We would map the attacks to individual tasks and task sequences being performed by the cyber defender at the time of the attack and allow the model to reflect the cyber defender responses. Once built and tested, the models could then be exercised to examine the sensitivity of the base task flows to the CEMA effects as well as assessing the outcomes to the changes in the task flows.

5. SUMMARY AND CONCLUSIONS

In this report we reviewed the CEMA threats and attacks that can impact human performance and developed initial approaches to integrate these impacts into human performance models. Since many of the threats, attacks, and impacts are dependent on the context of their use and what or who is targeted, we provided a framework for the development of scenarios for building and exercising human performance models that incorporate the CEMA threats, attacks, and impacts, with a focus on cyber defense operations and the cyber defense analyst.

Basic findings are as follows:

- *Task Performance.* CEMA attacks most often impact what tasks are performed when by cyber defenders. These kinds of effects can be incorporated into human performance models by elaborating on baseline task performance models to include a greater range of, or more detailed, attack detection, response, and recovery tasks, task flows, and branching logics, as well as inclusion of erroneous response tasks and probabilities of their occurrence.
- *Physical Harms* can result in harm to the targeted individual(s), harm to equipment or information, and potential for secondary psychological, reputational, or social/societal harm.
    - Harm to equipment or information results in changes to the tasks and actions the targets can take to further their goals or mitigate the effects of the attack.
    - The most common physical harm to targeted individuals from electromagnetic effects is some level of heating to either surface or internal tissues. The human eye is especially vulnerable across the spectrum but is at highest risk from nonvisible radiations. The effects to performance range from low levels of irritation to incapacitation at higher energy levels, and when implemented in nonlethal weapons. These effects can be implanted in models as performance time degradations, interference to decision-making tasks, and outright task interruptions.
- *Psychological Harms* can disrupt the ability of the targeted people to perform their tasks or pursue their intended goals due to psychological stress, which can interfere with decision making, task performance, and in extreme cases result in emotional trauma.
    - It is useful to think about them in terms of those that occur pre-attack-event and those that occur post-attack-event. Pre-attack, the attacker is trying to deceive or misdirect the CEMA defender, or even promote desired defender actions. A key area of human vulnerability in this phase is defender decision making and decision-making biases that can be exploited.

- Post-attack, the same decision-making considerations as pre-attack-detection are in play, but they are now subject to the emotional responses of the defender, and this emotional stress can exacerbate the impacts on decision making.
- Unless there has been training to avoid the bias, good cognitive discipline is expected, or other protective mechanisms are in place (e.g., default action), the literature suggests that most of these biases are likely to occur.
- With regard to consequences, these are typically reflected in human performance models by changes in task times or alternate decisions that result in different task actions from the baseline or desired task flow.
- Stress effects, to be useful in human performance modeling, need to be put in the context of what type of decision is being made, what biases are already associated with the decision, the likely defender perception of the stressor, and the general context in which the decision is being made. More novel or unexpected stressors will generally increase task performance time. More highly trained defenders and the presence of protective mechanisms will mitigate the impact of stress. Otherwise, stress will result in some increase in the effects of the biases associated with the task.

Modeling the effects of CEMA on human performance requires a scenario or set of scenarios that cover the range of CEMA performance effects as well as realistic operational scenarios that include a robust set of cyber defender tasks. It also requires a mapping of the effects to the tasks and the impact of those effects on the tasks. There are a number of CEMA scenarios already developed that can be used to support the development of an overarching scenario for human performance modeling. We also believe it would be very beneficial to align with any available CEMA training scenarios that could help support model validation.

6. REFERENCES AND DOCUMENTS

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *0*(0), 1–15.

Barth, A., Winker, R., Ponocny-Seliger, E., Mayrhofer, W., Ponocny, I., Sauter, C., & Vana, N. (2008). A meta-analysis of neurobehavioral effects due to electromagnetic field exposure emitted by GSM mobile phones. *Occupational & Environmental Medicine*, *65*(5).

Blick, D. W., Adair, E. R., Hurt, W. D., Sherry, C. J., Walters, T. J., & Merritt, J. H. (1997). Thresholds of microwave-evoked warmth sensations in human skin. *Bioelectromagnetics, 18*, 403–409.

Bonneville, L. (2016). *The SAS 1983-2014 (Elite)*. Oxford, UK: Osprey Publishing.

Bruce, R. (2016). *The US Navy's electric weaponry.* Retrieved from http://www.sadefensejournal.com/wp/the-us-navys-electric-weaponry/

Casey, T. (2007, September). *Threat agent library helps identify information security risks* (White Paper). Washington, DC: Intel Corporation.

Cesarini, J. (2012). The sun and ultraviolet radiation. In A. Perrin & P. Souques (Eds.), *Electromagnetic fields, environment and health* (Chapter 10). Paris, France: Springer-Verlag France.

Cohen, H., Kozlovsky, N., Richter-Levin, G., & Zohar, J. (2010). Post traumatic stress disorder in animal models. In H. Sore, A. Freidman, & D. Kaufer (Eds.), *Stress – From molecules to behavior: A comprehensive analysis of the neurobiology of stress responses* (p. 263). Weinheim, Germany: Wiley-VCH.

Courant, D. (2012). Lasers. In A. Perrin & P. Souques (Eds.), *Electromagnetic fields, environment and health* (Chapter 1). Paris, France: Springer-Verlag France.

Court, L. (2012a). Infrared radiation. In A. Perrin & P. Souques (Eds.), *Electromagnetic fields, environment and health* (Chapter 8). Paris, France: Springer-Verlag France.

Court, L. (2012b). Light and visible radiation. In A. Perrin & P. Souques (Eds.), *Electromagnetic fields, environment and health* (Chapter 9). Paris, France: Springer-Verlag France.

Curcio, G., Ferrara, M., Gennaro, L. D., Cristiani, R., D'Inzeo, G., & Bertini, M. (2004). Time-course of EMF effects on human performance and tympanic temperature. *Cognitive Neuroscience and Neuropsychology*, *15*(1).

Deniz, O. G., Kaplan, S., Selcuk, M. B., Terzi, M., Altun, G., Yurt, K. K., Aslan, K., & Davis, D. (2017). Effects of short and long term electromagnetic fields exposure on the human hippocampus. *Journal of Microscopy and Ultrastructure*, *5*(4).

Department of the Army. (2017). *Field manual No. 3-12: cyberspace and electronic warfare operations* (FM 3-12). Washington, DC: Headquarters, Department of the Army.

Department of the Army. (2018). Noise and vibration in Army Aviation. In *Aeromedical training for flight personnel* (TC 3-04.93) (Chapter 7). Washington, DC: Headquarters, Department of the Army.

Department of Defense. (2012). *Design criteria standard-human engineering* (MIL-STD-1472G). Philadelphia, PA: Navy Publishing and Printing Office.

Department of Homeland Security: Science and Technology Directorate. (2007, July). *Enough to make you sick: Suspect-subduing 'lightsaber'*. Retrieved from https://www.dhs.gov/science-and-technology/enough-make-you-sick

Duggan, P. (2017 April 30). Tactical CEMA in cognitive spaces. *Small Wars Journal*. Retrieved from https://smallwarsjournal.com/jrnl/art/tactical-cema-in-cognitive-spaces

Federal Communications Commission. (2012, March 6). *FCC enforcement advisory cell jammers, GPS jammers, and other jamming devices consumer alert: Using or importing jammers is illegal* (Enforcement Advisory No. 2012-02). Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/DA-12-347A1.pdf

Frey, A. H. (1962). Human auditory system response to modulated electromagnetic energy. *Journal of Applied Physiology*, *17*(4), 689–692.

Gavin, F. J. (2017). Crisis, instability, and preemption. In G. Perkovich, & A. E. Levite (Eds.). *Understanding cyber conflict*. Washington, D. C. Georgetown University Press.

Gillis, J. S. (1993). Effects of life stress and dysphoria on complex judgments. *Psychological Reports*, *72*, 1355–1363.

Gok, K., & Atsan, N. (2016). Decision-making under stress and its implications for managerial decision-making: A review of literature. *International Journal of Business and Social Research*. *6*(3), 38–47.

Hancock, P., Conway, G., Szalma, J., Ross, J., & Saxton, B. (2006). *A meta-analysis of noise effects on operator performance for IMPRINT*. Orlando, FL: University of Central Florida.

Harris, M. (2009, May 27). *US cops and military to get laser guns*. Retrieved from https://www.techradar.com/news/world-of-tech/us-cops-and-military-to-get-laser-guns-602983

Husseini, T. (2019, April 1*). HEL on high water: The top Navy laser weapon systems*. Retrieved from https://www.naval-technology.com/features/navy-laser-weapon-systems/

Institute of Electrical and Electronic Engineers. (2006, April 19). *C95.1-2005 IEEE standard for safety levels with respect to human exposure to radio frequency electromagnetic fields, 3 kHz to 300 GHz*. New York, NY: IEEE.

International Commission on Non-Ionizing Radiation Protection (ICNIRP). (2004). Guidelines on limits of exposure to ultraviolet radiation of wavelengths between 180 nm and 400 nm (Incoherent optical radiation). *Health Physics 87*(2).

Issitt, M. L. (2018). Fallacies, bias, and the post-truth mind. In *Alternative facts, post-truth and the information war* (pp. 104–105). Amenia, NY: Grey House Publishing.

Johnston, S. A., & D'Andrea, J. A. (2007). Behavioral and cognitive effects of electromagnetic field exposures. In F. S. Barns. & B. Greenebaum (Eds.). *Biological and medical aspects of electromagnetic fields* (Chapter 4). Philadelphia, PA: Taylor & Francis.

Kahneman, D. (2011). *Thinking fast and slow*. New York, NY: Farrar, Straus and Giroux. .

Kheifets, L., & Shimkhada, R. (2007). Epidemiologic studies of extremely low-frequency electromagnetic fields. In F. S. Barns. & B. Greenebaum (Eds.), *Biological and medical aspects of electromagnetic fields* (Chapter 6). . Philadelphia, PA: Taylor & Francis.

Kowalski, K. M., & Vaught, C. (2003). Judgement and decision-making under stress: An overview for emergency managers. *International Journal of Emergency Management*, *1*(3), 278–289.

LeBlanc, V. R. (2009). The effects of acute stress on performance: Implications for health professional education. *Academic Medicine*, *84*(10), 25–33.

LeVine, S. (2009). *The active denial system: a revolutionary, non-lethal weapon for today's battlefield* (DTP-065). Washington, DC: National Defense University Press.

Lindberg, B., Hamilton, S., Lebiednik, B., & Hager, K. (2018, July 27). Cyber integrating architecture. Small Wars Journal. Retrieved from https://smallwarsjournal.com/jrnl/art/cyber-integrating-architecture

Lockheed Martin Corporation (2015). *Gaining the advantage: Applying cyber kill chain® methodology to network defense*. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Marin, M. F., Shrmek, T. E., Maheu, F. S., & Lupien, S. J. (2010). Stress, emotion, and memory: the good, the bad, and the intriguing. In H. Soreq, A. Freidman, & D. Kaufer, D. (Eds.). *Stress – From molecules to behavior: A comprehensive analysis of the neurobiology of stress responses* (p. 167). Weinheim, Germany: Wiley-VCH.

Mason, J. W. (1968). A review of psychoendocrine research on the sympathetic-adrenal medullary system. *Psychom. Med*., *30* (Suppl.), 631–653.

Melnick, J. (2018, May 15). *Top 10 most common types of cyber attacks*. Retrieved from https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

Navy Environmental Health Center. (1992). *Ultraviolet radiation guide*. https://www.med.navy.mil/sites/nmcphc/Documents/policy-and-instruction/ih-ultraviolet-radiation-technical-guide.pdf

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National initiative for cybersecurity education (NICE) cybersecurity workforce framework* (NIST Special Publication 800-181). Gaithersburg, MD: National Institute of Standards and Technology.

Olson, H. (1967). *Music, physics and engineering*. Princeton, NJ: Dover Publications.

Osborn, K. (2007, April 5). Airman injured in heat-beam test. *ArmyTimes*.

Pols, P. (2017). *The unified kill chain: Designing a unified kill chain for analyzing, comparing and defending against cyber-attacks*. Retrieved from https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf

Rehn, K. W. & Riggs, P. K. (2002, May). *Non-lethal swimmer neutralization study* (Technical Document 3138). San Diego, CA: Space and Naval Warfare Systems Center.

Reynolds, T. (2005). *Ultrasound physics*. Phoenix, AZ: School of Cardiac Ultrasound, Arizona Heart Foundation.

Sanger, D. (2017). *Cyber, drones, and secrecy*. In Perkovich, G., & Levite, A. E. (Eds.) Understanding cyber conflict. Washington, DC: Georgetown University Press.

Schmidt, N., Richey, J., Zvolensky, M., & Maner, J. (2008 September). Exploring human freeze responses to a threat stressor. *J Behav Ther Exp Psychiatry*, *39*(3), 292–304.

Soreq, H., Friedman, A., & Kaufer, D. (Eds.). (2010). *Stress – From molecules to behavior: A comprehensive analysis of the neurobiology of stress responses*. Weinheim, Germany: Wiley-VCH.

Valentini, E., Ferrara, M., Presaghi, F., DeGennaro, L., & Curcio, G. (2010). A systematic review and meta-analysis of psychomotor effects of mobile phone electromagnetic fields. *Occupational & Environmental Medicine*, *67*(10).

Walters, T., Blick, D., Johnson, L., Adair, E., & Foster, K. (2000). Heating and pain sensation produced in human skin by millimeter waves: comparison to a simple thermal model. *Health Physics*, *78*(3), 259–267.

Yamakawa, K., Ohira, H., Matsunaga, M., & Isowa, T. (2016). Prolonged effects of acute stress on decision-making under risk: A human psychophysiological study. *Frontiers in Human Neuroscience*, *10*(444), 1–11.

Appendix A – List of Acronyms

ADS	Active Denial System
CEMA	cyber and electromagnetic activities
DCO	Defensive Cyberspace Operations
DCO-IDM	Defensive Cyberspace Operations-Internal Defensive Measures
DCO-RA	Defensive Cyberspace Operations-Response Action
DDoS	distributed denial-of-service
DODIN	Department of Defense Information Network
DoS	denial-of-service
GPS	global positioning system
HEL	high-energy laser
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	intrusion detection system
IP	Internet Protocol
KSA	Knowledge, Skills, and Abilities
LED	light-emitting diode
MD	message digest
MitM	man-in-the-middle
MPE	Maximum Permissible Exposure
NICE	National Initiative for Cybersecurity Education
OCO	Offensive Cyberspace Operations
OS	operating system

PHP	PHP: Hypertext Preprocessor
SPTA	spatial peak-temporal average
SQL	Structured Query Language
TCP	Transmission Control Protocol
USB	Universal Serial Bus
UV	ultraviolet
XSS	cross-site scripting

Appendix B – Common Cyber Attacks

This appendix provides further details on the most common types of cyber attacks as described by Melnick (2018).

Type/Subtype	Description
Denial-of-service (DoS)	A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests.
Distributed Denial-of-Service (DDoS)	A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.
DoS - TCP SYN Flood Attack	An attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker's device floods the target system's small in-process queue with connection requests, but it does not respond when the target system replies to those requests. This causes the target system to time out while waiting for the response from the attacker's device, which makes the system crash or become unusable when the connection queue fills up.
DoS - Teardrop Attack	This attack causes the length and fragmentation offset fields in sequential Internet Protocol (IP) packets to overlap one another on the attacked host; the attacked system attempts to reconstruct packets during the process but fails. The target system then becomes confused and crashes.
DoS - Smurf Attack	This attack involves using IP spoofing and the ICMP to saturate a target network with traffic. This attack method uses ICMP echo requests targeted at broadcast IP addresses. These ICMP requests originate from a spoofed "victim" address. This process is repeatable, and can be automated to generate huge amounts of network congestion.
DoS - Ping of Death Attack	This type of attack uses IP packets to 'ping a target system with an IP size over the maximum of 65,535 bytes. IP packets of this size are not allowed, so attacker fragments the IP packet. Once the target system reassembles the packet, it can experience buffer overflows and other crashes.
DDoS - Botnets	Botnets are the millions of systems infected with malware under hacker control in order to carry out DDoS attacks. These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system's bandwidth and processing capabilities. These DDoS attacks are difficult to trace because botnets are located in differing geographic locations.
Man-in-the-Middle (MitM) Attack	A MitM attack occurs when a hacker inserts itself between the communications of a client and a server.
MitM - Session Hijacking	In this type of MitM attack, an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client.
MitM - IP Spoofing	IP spoofing is used by an attacker to convince a system that it is communicating with a known, trusted entity and provide the attacker with access to the system. The attacker sends a packet with the IP source address of a known, trusted host instead of its own IP source address to a target host. The target host might accept the packet and act upon it.
MitM - Replay	A replay attack occurs when an attacker intercepts and saves old messages and then tries to send them later, impersonating one of the participants.

Type/Subtype	Description
Phishing Attack	Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery. It could involve an attachment to an email that loads malware onto your computer. It could also be a link to an illegitimate website that can trick you into downloading malware or handing over your personal information.
Spear Phishing Attack	Spear phishing is a very targeted type of phishing activity. Attackers take the time to conduct research into targets and create messages that are personal and relevant. Because of this, spear phishing can be very hard to identify and even harder to defend against. One of the simplest ways that a hacker can conduct a spear phishing attack is email spoofing, which is when the information in the "From" section of the email is falsified, making it appear as if it is coming from someone you know, such as your management or your partner company. Another technique that scammers use to add credibility to their story is website cloning — they copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials.
Drive-By Attack	Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window. Unlike many other types of cyber security attacks, a drive-by doesn't rely on a user to do anything to actively enable the attack — you don't have to click a download button or open a malicious email attachment to become infected. A drive-by download can take advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or lack of updates.
Password Attack	Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach. Access to a person's password can be obtained by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing.
Password Attack – Brute Force Guessing	Brute-force password guessing means using a random approach by trying different passwords and hoping that one works. Some logic can be applied by trying passwords related to the person's name, job title, hobbies or similar items.
Password Attack – Dictionary Guessing	A dictionary of common passwords is used to attempt to gain access to a user's computer and network.
SQL Injection Attack	SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data-plane input (for example, instead of the login or password) in order to run predefined SQL commands. A successful SQL injection exploit can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database, recover the content of a given file, and, in some cases, issue commands to the operating system.

Type/Subtype	Description
Cross-Site Scripting (XSS) Attack	XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application. Specifically, the attacker injects a payload with malicious JavaScript into a website's database. When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script. The most dangerous consequences occur when XSS is used to exploit additional vulnerabilities. These vulnerabilities can enable an attacker to not only steal cookies, but also log key strokes, capture screenshots, discover and collect network information, and remotely access and control the victim's machine.
Eavesdropping Attack	Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network.
Eavesdropping Attack - Passive	A hacker detects the information by listening to the message transmission in the network.
Eavesdropping Attack - Active	A hacker actively grabs the information by disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning or tampering.
Birthday Attack	Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature. A message processed by a hash function produces a message digest (MD) of fixed length, independent of the length of the input message; this MD uniquely characterizes the message. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. If an attacker calculates same MD for his message as the user has, he can safely replace the user's message with his, and the receiver will not be able to detect the replacement even if he compares MDs.
Malware Attack	Malicious software can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet.
Malware Attack - Macro Viruses	These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.
Malware Attack - File Infectors	File infector viruses usually attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded. Another version of a file infector associates itself with a file by creating a virus file with the same name, but an .exe extension. Therefore, when the file is opened, the virus code will execute.
Malware Attack - System or Boot-Record Infectors	A boot-record virus attaches to the master boot record on hard disks. When the system is started, it will look at the boot sector and load the virus into memory, where it can propagate to other disks and computers.
Malware Attack - Polymorphic Viruses	These viruses conceal themselves through varying cycles of encryption and decryption. The encrypted virus and an associated mutation engine are initially decrypted by a decryption program. The virus proceeds to infect an area of code. The mutation engine then develops a new decryption routine and the virus encrypts the mutation engine and a copy of the virus with an algorithm corresponding to the new decryption routine. The encrypted package of mutation engine and virus is attached to new code, and the process repeats. Such viruses are difficult to detect but have a high level of entropy because of the many modifications of their source code.

Type/Subtype	Description
Malware Attack - Stealth Viruses	Stealth viruses take over system functions to conceal themselves. They do this by compromising malware detection software so that the software will report an infected area as being uninfected. These viruses conceal any increase in the size of an infected file or changes to the file's date and time of last modification.
Malware Attack - Trojans	A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers.
Malware Attack - Logic Bombs	A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.
Malware Attack - Worms	Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. Worms are commonly spread through email attachments; opening the attachment activates the worm program. A typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address. In addition to conducting malicious activities, a worm spreading across the Internet and overloading email servers can result in denial-of-service attacks against nodes on the network.
Malware Attack - Droppers	A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the Internet and download updates to virus software that is resident on a compromised system.
Malware Attack - Ransomware	Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key.
Malware Attack - Adware	Adware is a software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up windows or through a bar that appears on the computer screen automatically.
Malware Attack - Spyware	Spyware is a type of program that is installed to collect information about users, their computers or their browsing habits. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the Internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.

Appendix C – Common Electromagnetic Effect Attacks

This appendix provides further details on the electromagnetic effect attacks as described Lindberg et al. (2018) and supplemented by Department of the Army (2017).

Kill Chain Step/Attack	Description
Reconnaissance	
Radio Frequency Identification	The measurement of the frequency at which a received signal was transmitted with the intent of uniquely identifying the source.
Radio Frequency Direction Finding	The measurement of the direction from which a received signal was transmitted.
Denial of Service	
Electromagnetic Jamming	The deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. Examples of targets subject to jamming include radios, radars, navigational aids, satellites, and electro-optics.
Electro-Optical-Infrared Jamming	A device or technique employing electro-optical-infrared materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision-guided weapons and sensor systems. Electro-optical-infrared countermeasures may use laser jammers, obscurants, aerosols, signature suppressants, decoys, pyrotechnics, pyrophorics, high-energy lasers, or directed infrared energy countermeasures.
Radio Frequency Jamming	Any device or technique employing radio frequency materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision-guided weapons and sensor systems. Radio frequency countermeasures can be active or passive. Expendable jammers used by aircraft to defend against precision-guided surface-to-air missile systems are an example of radio frequency countermeasures.
Electromagnetic Pulse	The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. An electromagnetic pulse induces high currents and voltages in the target system, damaging electrical equipment or disrupting its function. An indirect effect of an electromagnetic pulse can be electrical fires caused by the heating of electrical components.
Initial Entry	
Electronic Probing	Intentional radiation designed to be introduced into the devices or systems of potential enemies for the purpose of learning the functions and operational capabilities of the devices or systems.
Obtaining Stolen Certificates	Self-evident
Exploiting unencrypted messages	Self-evident
Privilege Escalation	N/A

Kill Chain Step/Attack	Description
Data Manipulation	
Man-in-the-Middle Attack	When the attacker inserts themselves into the communication streams of the target. The next four attacks that follow are all variations on the man-in-the-middle attack.
Message Spoofing	Inserting a false message in the communication stream
GPS Spoofing	Inserting a false GPS location in the communications stream
Electromagnetic Deception	The deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Types of electromagnetic deception include manipulative, simulative, and imitative. Manipulative involves actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces. Simulative involves actions to simulate friendly, notional, or actual capabilities to mislead hostile forces. Imitative introduces electromagnetic energy into enemy systems that imitates enemy emissions.
Electromagnetic Intrusion	The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. Electromagnetic intrusion is often conducted by inserting false information. This information may consist of voice instructions, false targets, coordinates for fire missions, or rebroadcasting prerecorded data transmissions.
Persistence	
Beaconing Using the Electromagnetic Spectrum	The infected host computer is communicating to the malware command and control computers at regular intervals using the electromagnetic spectrum most commonly through a host communications capability.

Appendix D – Electromagnetic Effects on Human Performance

This appendix is presented as a series of fact sheets broken down by spectrum and frequency range as given in Table D-1 with the exception of gamma and X-rays. Each spectrum range includes a list of example sources, uses, biological and human performance effects, example weapon system(s) when available, and a discussion of the application to human performance modeling.

Table D-1. Electromagnetic Spectrum

Electromagnetic spectrum			
Name	**Wavelength**	**Frequency (Hz)**	**Photon energy (eV)**
Gamma ray	<0.02 nm	>15 EHz	>62.1 keV
X-ray	0.01 nm–10 nm	30 EHz–0 PHz	124 keV–124 eV
Ultraviolet	10 nm–400 nm	30 PHz–750 THz	124 eV–3 eV
Visible light	390 nm–750 nm	770 THz–400 THz	3.2 eV–1.7 eV
Infrared	750 nm–1 mm	400 THz–300 GHz	1.7 eV–1.24 meV
Microwave	1 mm–1 m	300 GHz–300 MHz	1.24 meV–1.24 μeV
Radio	1 mm–100 km	300 MHz–3 kHz	1.24 μeV–12.4 feV
Sonic	N/A	10 KHz–0 Hz	N/A

D.1 Ultraviolet Radiation: 750 THz–30 PHz

Ultraviolet (UV) radiation comprises the spectrum frequencies between visible light and ionizing radiation (X-ray and gamma ray). It is present in sunlight and contributes about 10% of the total output of the Sun.

Sources/Uses

- Sun
    - Mostly filtered by the Earth's atmosphere
    - Triggers the body to produce vitamin D
- Lamps (incandescent, low-pressure discharge, fluorescent, tanning, germicidal)
- High-intensity discharge
- Black lights
- Arc welding
- Spectrometry

Biological Effects

The effects all require periods of exposure and latency periods between exposure and the occurrence of symptoms. Effects include the following (Cesarini, 2012; Navy Environmental Health Center, 1992):

- Erythema (sunburn) symptoms range from skin reddening to serious burns and has a latency period of 4–8 h.
- Skin photosensitization when certain materials are in contact with the skin during UV exposure (pitch, petroleum, coal tar, and dyes).
- Acute kerato-conjunctivitis (snow blindness or welder's flash) results from excessive exposure of the cornea to UV. Symptoms can be extremely painful with a latency period of 4–12 h but usually last for less than 24 h. Symptoms include a sensation of sand in the eyes, photophobia, blurred vision, and uncontrolled excessive blinking. Full recovery can take a couple days.
- Long-term effects include skin aging, cataracts, and certain types of skin and eye cancers can result from extended periods of exposure over many years.

Weapon System Examples

No example weapons systems using the UV spectrum, other than lasers, have been included in this review.

Human Performance Modeling

The latency periods suggest that most symptoms take hours to occur but can result in visual and pain performance limitations lasting for several hours. Several safety standards have been developed showing a wide range of exposure limits (ICNIRP, 2004). A modeling algorithm could be created to represent the occurrence of symptoms in personnel given exposure situations. The level of human performance degradation would likely be a function of irritation or injury and could result in task performance effects or personnel availability issues.

D.2 Visible: 770 THz–400 THz

Visible light is the portion of the spectrum defined by its accessibility to the human visual system. Light is an essential condition for life on the surface of the Earth.

Sources/Uses

- The Sun
- Welding arcs
- Lamps
- LED
- High-intensity spotlight
- Human vision
- Photosynthesis

Biological Effects

Pupil dilation and the blink response limit the effects of visible light to structures of the eye. Thermal effects can occur if the tissue temperature increases fast enough. Photochemical effects can occur in the range of 400–700 nm known as blue light (Court, 2012b).

Weapon System Examples

Stun Grenade (Flashbang)

The stun grenade produces a blinding flash and intense loud "bang" to disorient the target's senses. The flash activates all the photoreceptor cells causing blindness for approximately 5 s and an afterimage that continues to impair vision. The loud blast causes temporary deafness and disturbs the fluid in the ear causing a loss of balance (Bonneville, 2016).

LED Incapacitator

Designed as a flashlight, it emits an extremely bright, rapid, and well-focused series of different-colored random pulses. Before the eye can focus on one frequency, it changes, causing intracranial pressure resulting in headaches, nausea, vomiting, disorientation, irritability, and visual impairment (Department of Homeland Security, 2007).

Human Performance Modeling

Algorithms could be developed for the temporary disabling effects of high-intensity visible light. The performance degradation would occur instantly upon exposure and cause task interruptions. Restarting a task would be a function of the effect duration.

D.3 Infrared: 300 GHz–400 THz

Infrared radiation consists of the spectrum frequencies between visible light and microwave and is generally invisible to the human eye. Most of the thermal radiation (heat) emitted by objects near room temperature is infrared.

Sources/Uses

- Sun
- Heating elements
- Telecommunications
- Heating in industrial applications
- Night vision
- Missile guidance
- Meteorology
- Climatology
- Astronomy
- Spectroscopy

Biological Effects

Thermal damage to eyes is rare as a rise in cornea temperature to 45 °C induces a pain response and avoidance reflex. Chronic exposure over years is observed to cause lesions and other ocular disorders. Thermal damage to the skin depends on incident temperature and exposure duration. The sensation of burning limits most exposures (Court, 2012a). Very high temperatures can cause serious burns in less than a second, while lower temperatures can cause as much damage during long exposures.

Weapon System Examples

No example weapons systems using the infrared spectrum, other than lasers, have been included in this review.

Human Performance Modeling

When exposed to a hot environment for extended periods the body's thermal equilibrium is perturbed. Human performance is affected by the physical and cognitive effects of being overheated. The effects of heat are well established and are included in modeling tools. The effects of burns are less clear. Serious burns will cause task interruptions and the unavailability of the individual to continue tasks. However, the performance effects of the range of less serious burns will depend on the portion of the anatomy affected.

D.4 Laser: 300 GHz–30 PHz

- Infrared (300 GHz–400 THz)
- Visible (400 THz–770 THz)
- UV (750 THz–30 PHz)

The word "laser" is an acronym for light amplification by stimulated emission of radiation. It refers to a device that emits light through optical amplification. It differs from other energy sources in that it can focus to a tight spot, stay narrow over great distances, and emit with a very narrow spectrum.

Sources/Uses

- Medical
- Commercial/manufacturing
- Communication
- Scanning
- Targeting/weapon
- Presentation

Biological Effects

The hazard only exists within the path of the beam, and effects vary depending on wavelength, power, duration, and portion of the anatomy affected. Eyes are especially susceptible to damage from highly focused light as they focus and concentrate the source to the retina. Visible light is somewhat less dangerous due to the blink response of less than a quarter of a second while nonvisible light could affect the eye over many seconds. The skin is less sensitive but burns of varying degrees will occur in the small tissue area of the beam (Courant, 2012).

Weapon System Examples

Dazzler

A dazzler is a nonlethal weapon using intense directed radiation to temporarily disable its target with flash blindness and is intended to cause no long-term damage to eyes (Harris, 2009). The emitters are usually lasers, but very bright searchlights have been used to disorient pilots. Contemporary systems are generally portable with effective ranges of up to 4 km. Systems can incapacitate from seconds to several minutes.

HEL – High-Energy Laser

Land-based and vehicle-mounted HELs are in the test phase. Capable of emitting a beam greater than 100 kW, they may be powerful enough to destroy cruise missiles, artillery rockets, and mortar rounds (Bruce, 2016; Husseini, 2019).

Human Performance Modeling

The spectrum range, source types, power levels, and physical effects for laser are extremely broad. Numerous exposure limits have been developed across industry and the military. It may be possible to create a laser effects component for modeling, but it will take considerable effort to determine which types out of the huge range will be appropriate.

D.5 Microwave Radiation: 300 MHz–100 GHz

Microwave radiation comprises the higher frequencies of the radio component of the electromagnetic spectrum. Unlike lower frequency radio waves, microwaves travel in line-of-sight.

Sources/Uses

- Telecommunication and broadcasting
- Point-to-point communication
- Radar and radio astronomy
- Satellite and spacecraft communication
- Energy transmission
- Wireless data transfer (cell, Bluetooth, etc.)
- Medical
- Microwave oven
- Industrial heating

Biological Effects

At higher energy levels, microwaves can produce surface and internal burns through dielectric heating (excitation of water molecules) such as a damaged microwave oven. There are also auditory effects (Johnston & D'Andrea, 2007). A wide range of studies and meta-analyses have been done to assess the effect of long-term cell phone use on human performance. Minor short-term effects but no long-term effects have been identified (Barth et al., 2008; Curcio, 2004; Deniz et al., 2017; Valentini, Ferrara, Presaghi, DeGennaro, & Curcio, 2010).

Weapon System Examples

Microwave Auditory Effect (Microwave hearing effect or Frey effect) (Frey, 1962)

Pulsed microwave radiation, from a distance of inches to hundreds of feet, can result in auditory effects such as "a buzz, clicking, hiss, or knocking". Apparently, an induced perception of severe buffeting of the head can also occur. The cause is thought to be thermostatic expansion of portions of auditory apparatus (rapid heating of brain by each pulse and resulting pressure wave traveling through the skull to the cochlea). A few weapon concepts have been researched but there is concern that the heating of tissues would result in brain damage or death.

Millimeter Wave Weapon (94–95 GHz)

When directed at a person, Active Denial System (ADS) (LeVine, 2009) causes heating of water and fat molecules in first 1/64 inch of the skin and cornea. Surface temperatures can reach levels

causing up to second-degree burns if exposed too long or at too high a power. The burns are similar to microwave burns but only affect the surface of the skin without the penetration of microwaves. The developers have been able to demonstrate a large enough delta between desired repel responses versus injury to consider it a reasonable safety limit (Blick et al., 1997). Higher power levels and longer durations can cause more serious burns (Osborn, 2007).

Human Performance Modeling

In the nonlethal configuration of ADS, personnel generally reach their tolerance limit within 3 and 5 s is unendurable. The response to leave the area of the beam during tests is reported as automatic or uncontrolled (repel response). In addition to the these anecdotal data, a thermal model has been developed based on the results of the test exposures that may be suitable developing a human performance modeling component (Walters, Blick, Johnson, Adair & Foster, 2000).

D.6 Radio Frequency: 3 KHz–300 MHz

Radio waves cover the electromagnetic spectrum with frequencies below infrared. For the purposes of this review, the microwave frequency of radio waves is listed separately, leaving the range from 3 KHz to 300 MHz for radio. Radio waves are generated by electric charges undergoing accelerations. Naturally occurring radio waves are emitted by lightning and astronomical objects.

Sources/Uses

- Lightning
- Semiconductor manufacturing tools
- Heaters
- Broadcasting
- Communications
- Radar
- Magnetic resonance imaging
- Defibrillators

Biological Effects

The primary effects are electrical burns and electric shocks. The severity ranges across the spectrum, the type of energy field, the power levels, and the portion of the anatomy affected. Extended exposures can result in carcinogenic effects including cancer (Kheifets & Shimkhada, 2007).

Weapon System Examples

Electroshock Weapons

An electroshock weapon delivers sufficient energy to disrupt muscle function and/or inflict pain. Many type of devises exist. Tasers (www.taser.com) are the most commonly recognized weapon that can be used at distance while stun guns and prods require direct application. In addition, several wireless versions have been developed that can function at much longer ranges than the wire-based version of the Taser. The effect durations are only a few seconds but a level of disorientation can last longer.

Radio Jamming

Radio jamming is a deliberate jamming, blocking, or interference with authorized wireless communications (Federal Communications Commission, 2012). Methods generally involved transmitting on the same frequency with higher power or a very noisy signal. Other methods interfere with receiver stations such as satellite communications. Iran has regularly used jamming to prevent its citizens from receiving radio signals from other countries and satellites. As recently as 2015, the United Nations has issued warnings about health effects to civilian populations up to and including cancer. These potential effects are based on long-term exposure.

Human Performance Modeling

The Institute of Electrical and Electronic Engineers has established a standard for Maximum Permissible Exposures (MPEs) for external electrical fields (Institute of Electrical and Electronic Engineers, 2006). Included are extremely detailed breakdowns of exposure limits by portions of the body, field types, frequencies, and power densities. The tables and graphs describing these limits could be adapted to modeling algorithms. Additional details on the duration and performance effects will need to be included. In addition, studies have demonstrated some cognitive effects to attention, vigilance, and memory (Johnston & D'Andrea, 2007).

D.7 Sound: 20 Hz–20 KHz

Sound is a vibration that propagates as an audible wave of pressure through a transmission medium. For animals, sound is the reception of such waves and their perception by the brain. Humans can hear sounds waves at frequencies between about 20 Hz and 20 kHz. Sounds waves above 20 kHz are known as ultrasound. Sounds waves below 20 Hz are known as infrasound (Olson, 1967).

Biological Effects

- Nausea
- Discomfort
- Extreme pain
- Disorientation
- Sufficient to incapacitate

There are no proven biological effects for unfocused sound beams with intensity below 100 mW/cm^2 spatial peak-temporal average (SPTA) or focused sound beams below intensity of 1 mW/cm^2 SPTA. High-intensity ultrasound has been shown to cause organ damage, cardiovascular effects, and muscle contraction (mouse studies). Other effects include vibrotactile sensitivity changes and vestibular balance effects (Reynolds, 2005). Injury to scuba divers can occur when exposed to low-frequency tones longer than 15 min as low-frequency sound passes easily from water to body. Injuries include immediate and long-term brain tissue damage similar to symptoms of suffering minor head injuries (Rehn & Riggs, 2002).

Weapon System Examples

Long-Range Acoustic Devices

Long-range acoustic devices (https://www.genasys.com) have been used to deter pirates and crowd control (protestors/rioters). Mobile sonic devices have been used to deter teenagers by emitting an ultra-high-frequency blast (19–20 kHz) that people under 20 find uncomfortable. Age-related hearing loss limits the effect in people in their late twenties and older. High-amplitude sound of specific patterns and frequency close to the sensitivity of human hearing (2–3 kHz) are used in burglar deterrent and other types of alarms.

Stun Grenade (Flashbang) (Bonneville, 2016)

The stun grenade produces a blinding flash and intense loud “bang” to disorient the target’s senses. The flash activates all the photoreceptor cells causing blindness for approximately 5 s and an afterimage that continues to impair vision. The loud blast causes temporary deafness and disturbs the fluid in the ear causing a loss of balance.

Human Performance Modeling

Injuries and effects based on decibel levels and a various hazard standards for noise are readily available (Department of the Army, 2018; Department of Defense, 2012). Performance effects to communication have already been included in modeling tools (Hancock, Conway, Szalma, Ross & Saxton, 2006). Additional modeling could be created for task interruptions based on temporary disorientation.

Appendix E – Distribution List

ORGANIZATION

U.S. Army CCDC Data & Analysis Center
FCDD-DAD-OL/T Handlir
FCDD-DAH-C/C Garneau
6896 Mauchly St.
Aberdeen Proving Ground, MD 21005-5071

Alion Science and Technology
C Plott

U.S. Army CCDC Army Research Laboratory
FCDD-RLD-CL/Tech Library
2800 Powder Mill Rd.
Adelphi, MD 20783

Defense Technical Information Center
ATTN: DTIC-O
8725 John J. Kingman Rd.
Fort Belvoir, VA 22060-6218