STRESS & HACKING

Understanding Cognitive Stress in Tactical Cyber Operations

Celeste Lyn Paul and Josiah Dykstra
National Security Agency

SPEAKERS

CELESTE LYN PAUL

Senior Researcher and Technical Advisor at NSA Research

Ph.D. in Human-Centered Computing

Hackers are people too

JOSIAH DYKSTRA

Deputy Technical Director of NSA Cybersecurity Operations

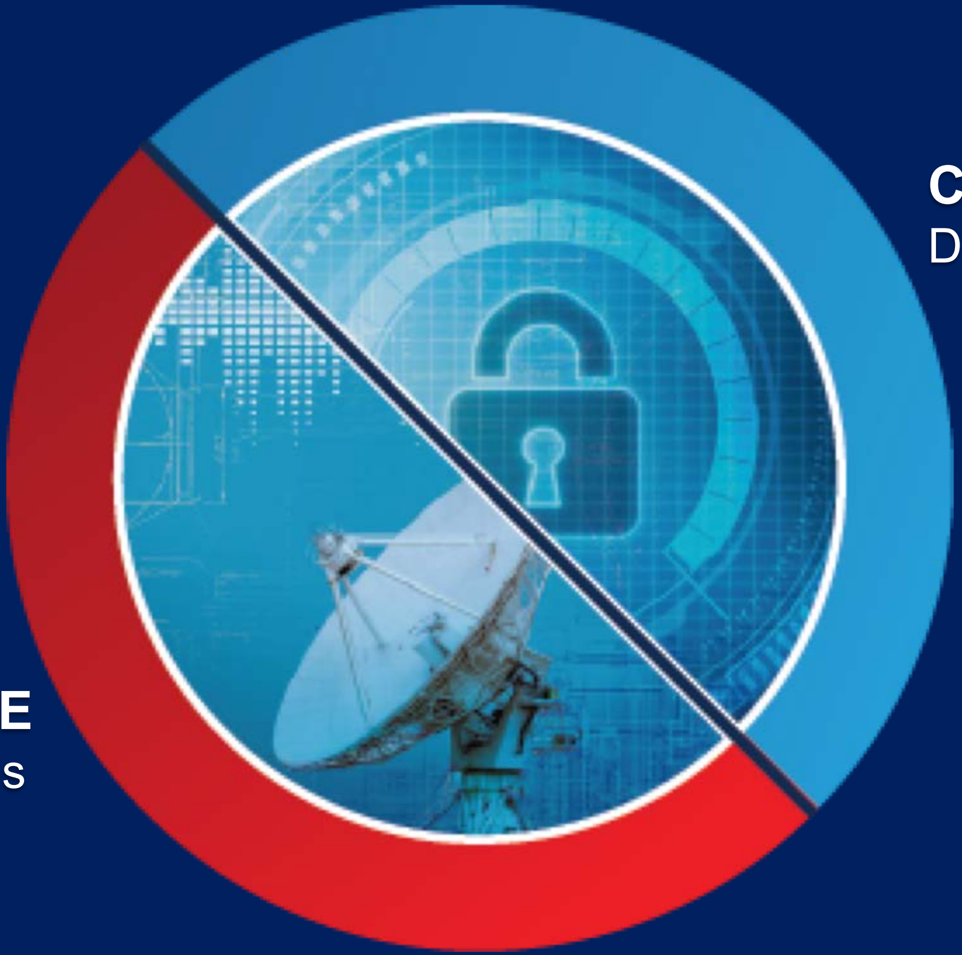
Ph.D. in Computer Science

Late to the party

AGENDA

- About NSA
- Tactical Cyber Operations
- Stress and Hacking at NSA
- Putting these Results to Work

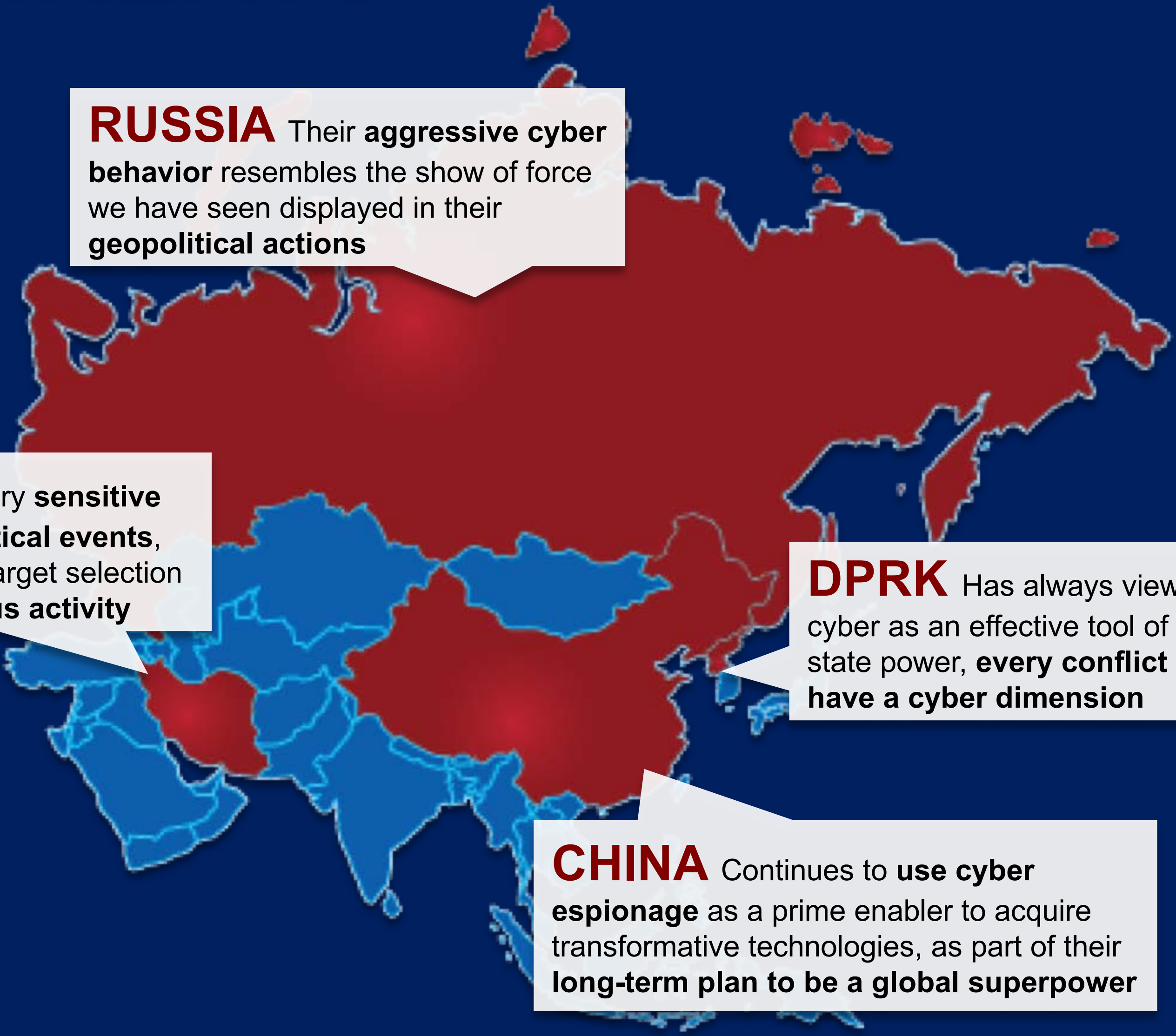
NATIONAL SECURITY AGENCY



CYBERSECURITY
Defend national security systems

SIGNALS INTELLIGENCE
Intercept and exploit foreign signals

CYBERTHREATS



RUSSIA Their **aggressive cyber behavior** resembles the show of force we have seen displayed in their **geopolitical actions**

IRAN Remains very **sensitive to international political events**, which can influence target selection and **level of malicious activity**

DPRK Has always viewed cyber as an effective tool of state power, **every conflict will have a cyber dimension**

CHINA Continues to **use cyber espionage** as a prime enabler to acquire transformative technologies, as part of their **long-term plan to be a global superpower**

PARTNERS

INTELLIGENCE COMMUNITY

INDUSTRY & ACADEMIA

COMBATANT COMMANDS

U.S. GOV. SECTORS

FOREIGN PARTNERS

LAW ENFORCEMENT
& COUNTER INTEL

NCTOC

National Cybersecurity Threat Operations Center

WHERE WE OPERATE

Computer Network Exploitation

ADVERSARY NETWORKS

U.S. GOV. NETWORKS

On-Network Operations

- Vulnerability Assessments
- Authorized Hacking
- Targeted Hunting
- Incident Response
- Comms Security Monitoring

DEPARTMENT OF DEFENSE INFORMATION NETWORK

STRESS & HACKING @ black hat USA 2018

Just before this talk:

Holding on for Tonight: Addiction in InfoSec

Now:

Stress and Hacking: Understanding Cognitive Stress in Tactical Cyber Operations

This afternoon:

Mental Health Hacks: Fighting Burnout, Depression and Suicide in the Hacker Community

Tomorrow morning:

Demystifying PTSD in the Cybersecurity Environment

Let’s talk about **stress**.

TYPES OF STRESS

ACUTE	Temporary ‘fight or flight’ response
EPISODIC	Repetitive stress with little time to recover
CHRONIC	Enduring situations with no sense of control

WHY IS HACKING SO STRESSFUL?

COMPLEX

UNPREDICTABLE

HIGH RISK / REWARD

STUDYING STRESS

- Hard to study
- Multi-faceted
- Dependent on environment
- Very subjective

STRESS HAS EFFECTS ON…

FATIGUE	Physical and mental feeling of tiredness
FRUSTRATION	Anxiety and annoyance over lack of control
COGNITIVE WORKLOAD	Amount of mental effort needed to use memory

FATIGUE

Samn-Perelli Fatigue Scale

Fatigue: How awake or tired are you before the operation?

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

Fully alert,
wide awake.

Very responsive,
but not at peak.

Okay, somewhat
fresh

A little tired, less
than fresh.

Moderately tired,
let down.

Extremely tired, very
difficult to concentrate.

Exhausted, unable to
function effectively

FRUSTRATION & COGNITIVE WORK

NASA Task Load Index (TLX)

Very Low Very High

□□□□□□□□□□□□□□□□□□□□

Mental Demand: How mentally demanding was the operation?

Physical Demand: How physically demanding was the operation?

Time Demand: How hurried or rushed was the pace of the operation?

Overall Performance: How successful were you in accomplishing what you were asked to do?

Frustration Level: How insecure, discouraged, irritated, stressed, and annoyed were you?

Effort: How hard did you have to work to accomplish your level of performance?

BASELINE

Normalizing Individual Differences

Fatigue: How awake or tired are you **before the operation**?

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

Fully alert, wide awake.	Very responsive, but not at peak.	Okay, somewhat fresh	A little tired, less than fresh.	Moderately tired, let down.	Extremely tired, very difficult to concentrate.	Exhausted, unable to function effectively

Fatigue: How awake or tired are you **after the operation**?

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

Fully alert, wide awake.	Very responsive, but not at peak.	Okay, somewhat fresh	A little tired, less than fresh.	Moderately tired, let down.	Extremely tired, very difficult to concentrate.	Exhausted, unable to function effectively

BASELINE

Normalizing Individual Differences

Frustration Level: How insecure, discouraged, irritated, stressed, and annoyed **are you**?

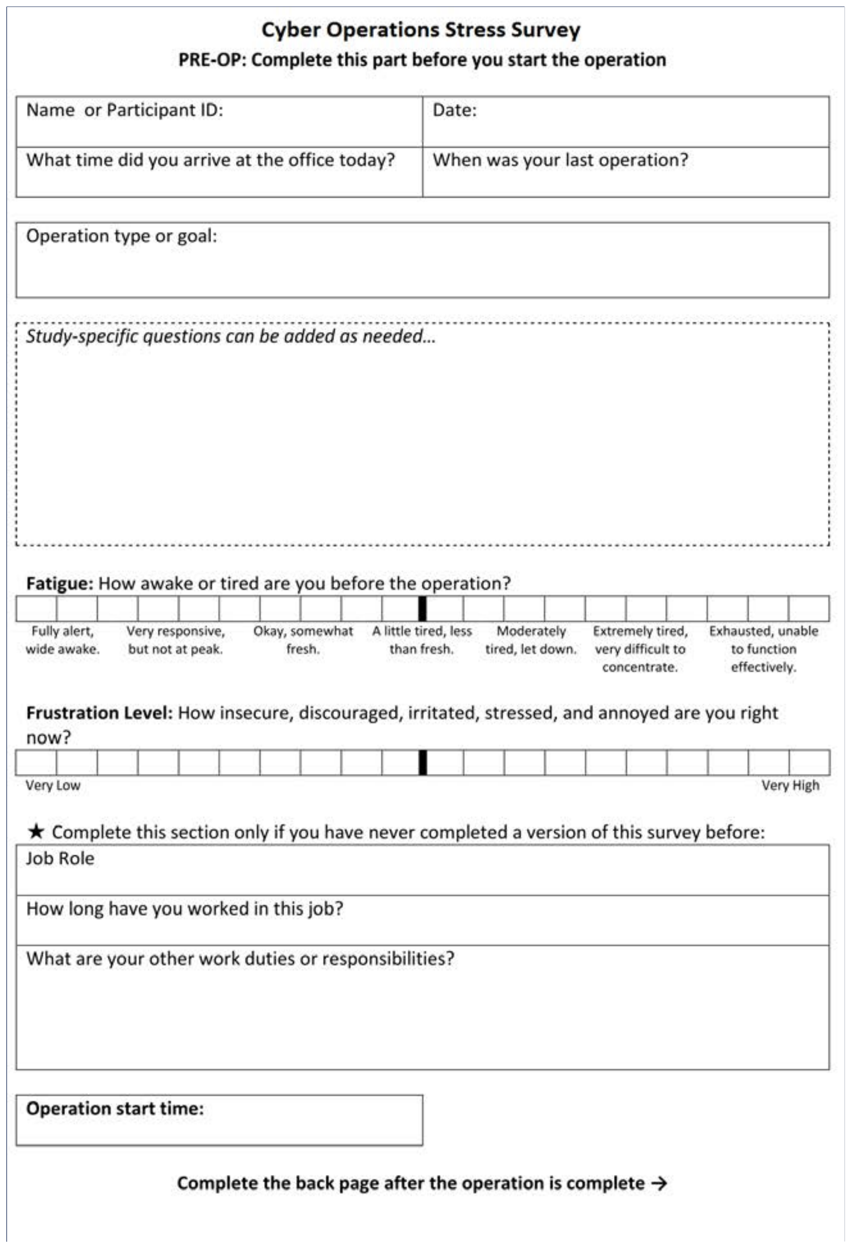
□□□□□□□□□□□□□□□□□□□□

Very Low Very High

Frustration Level: How insecure, discouraged, irritated, stressed, and annoyed **were you**?

□□□□□□□□□□□□□□□□□□□□

Very Low Very High



Cyber Operations Stress Survey

PRE-OP: Complete this part before you start the operation

Name or Participant ID:	Date:
What time did you arrive at the office today?	When was your last operation?

Operation type or goal:

Study-specific questions can be added as needed…

Fatigue: How awake or tired are you before the operation?

Fully alert, wide awake.	Very responsive, but not at peak.	Okay, somewhat fresh.	A little tired, less than fresh.	Moderately tired, let down.	Extremely tired, very difficult to concentrate.	Exhausted, unable to function effectively.

Frustration Level: How insecure, discouraged, irritated, stressed, and annoyed are you right now?

Very Low — Very High

★ Complete this section only if you have never completed a version of this survey before:

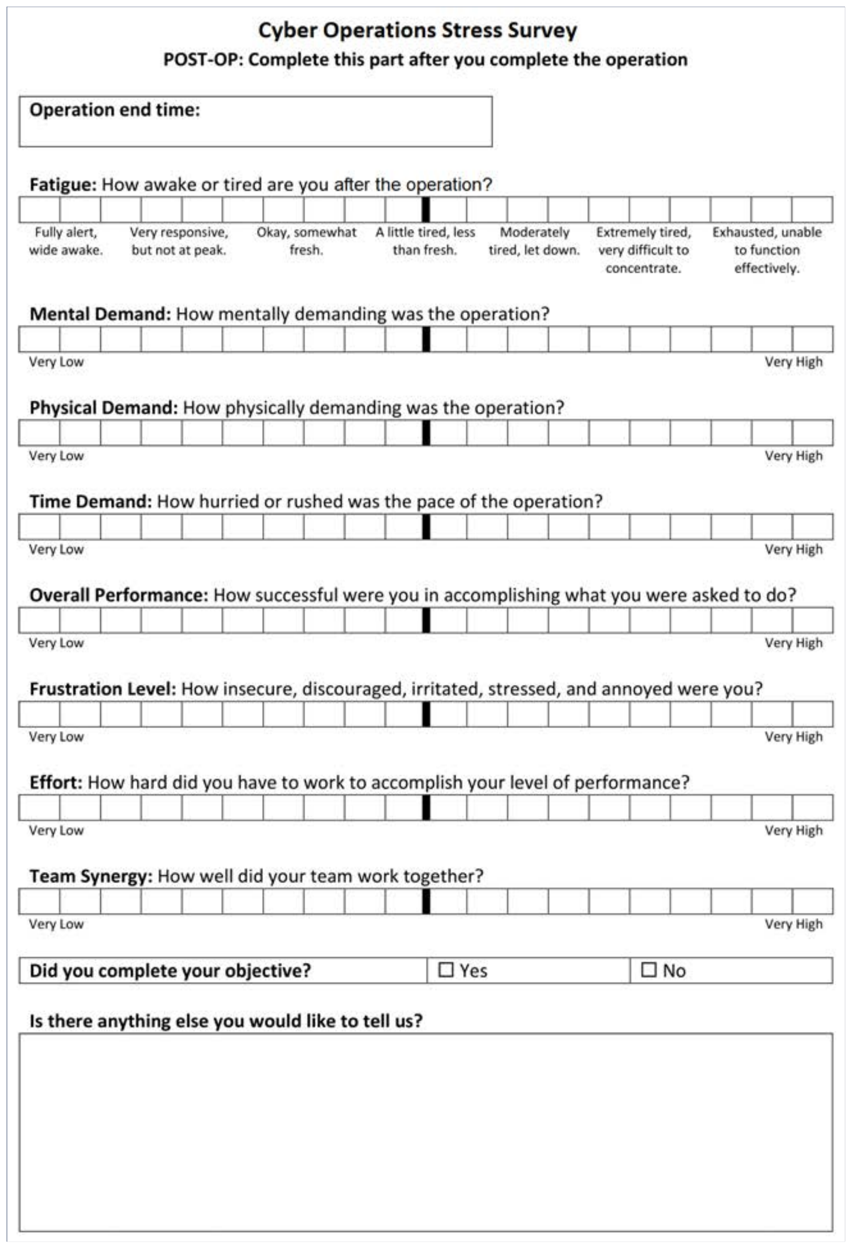
Job Role

How long have you worked in this job?

What are your other work duties or responsibilities?

Operation start time:

Complete the back page after the operation is complete →



Cyber Operations Stress Survey

POST-OP: Complete this part after you complete the operation

Operation end time:

Fatigue: How awake or tired are you after the operation?

Fully alert, wide awake.	Very responsive, but not at peak.	Okay, somewhat fresh.	A little tired, less than fresh.	Moderately tired, let down.	Extremely tired, very difficult to concentrate.	Exhausted, unable to function effectively.

Mental Demand: How mentally demanding was the operation?

Very Low — Very High

Physical Demand: How physically demanding was the operation?

Very Low — Very High

Time Demand: How hurried or rushed was the pace of the operation?

Very Low — Very High

Overall Performance: How successful were you in accomplishing what you were asked to do?

Very Low — Very High

Frustration Level: How insecure, discouraged, irritated, stressed, and annoyed were you?

Very Low — Very High

Effort: How hard did you have to work to accomplish your level of performance?

Very Low — Very High

Team Synergy: How well did your team work together?

Very Low — Very High

Did you complete your objective?	□ Yes	□ No

Is there anything else you would like to tell us?

ENTRANCE
CLOSED
RESERVED
Senior
PERMIT
REQUIRED

PARTICIPANTS

4 NSA Locations

126 Tactical Cyber Operators

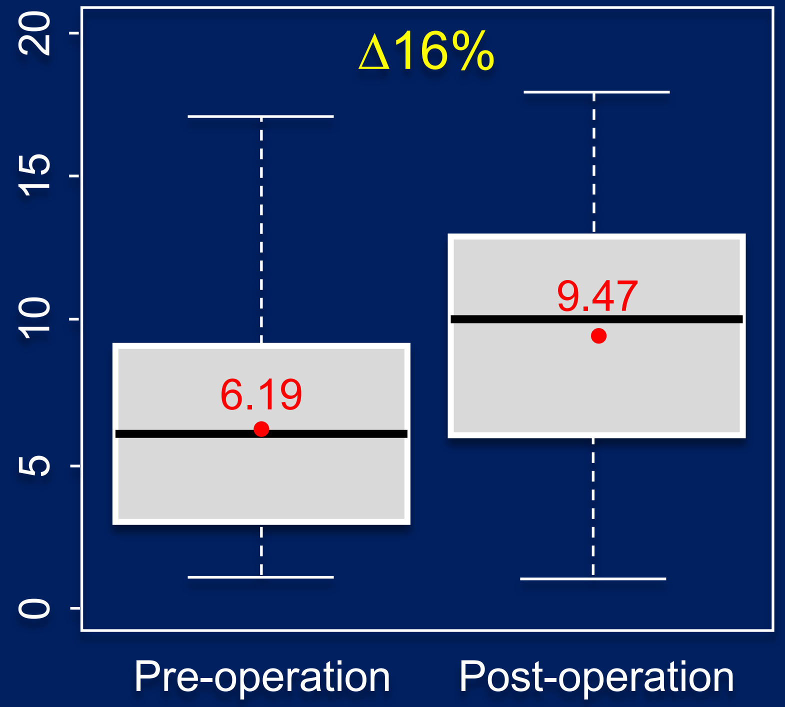
361 Operation Surveys

Both CIV and MIL*

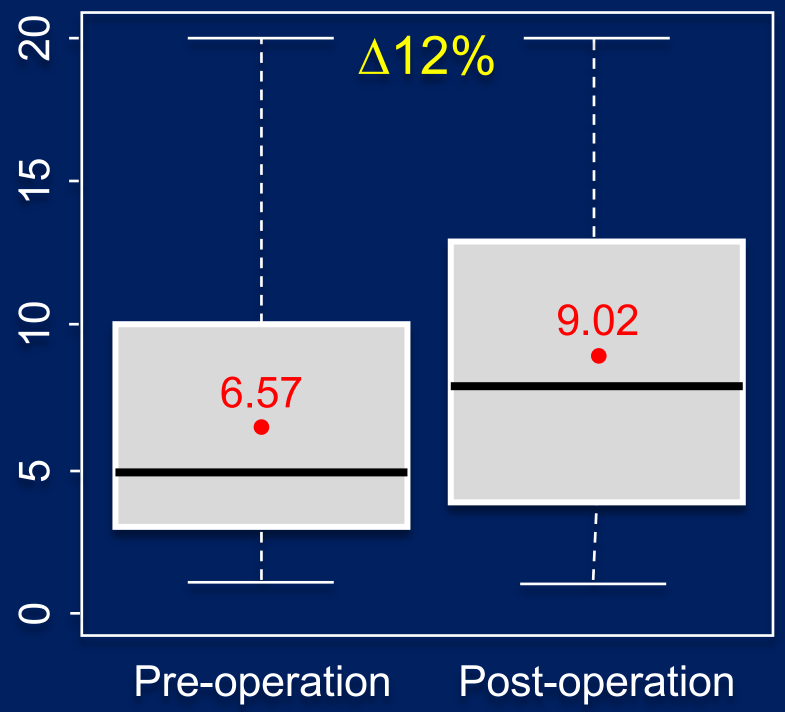
RESULTS

Tactical Cyber Operations cause stress.

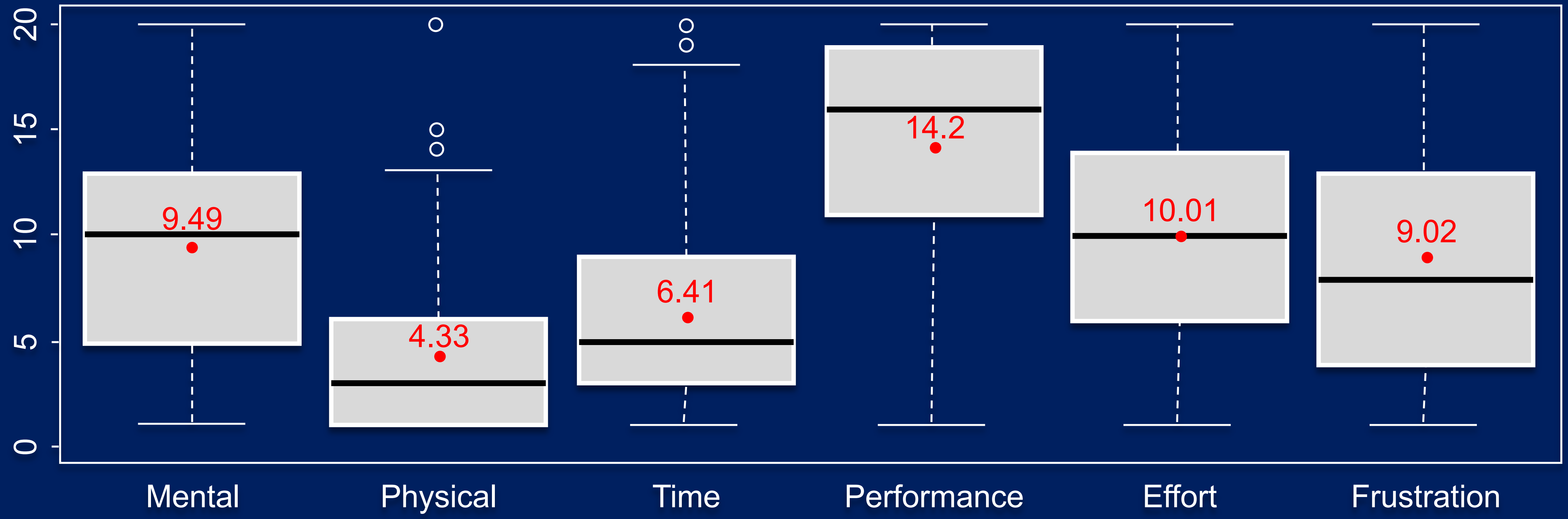
FATIGUE



FRUSTRATION



COGNITIVE WORKLOAD



RTLX = 44.5 (SD = 28.1)

Is this a lot?

Hint: That’s not the right question.

COGNITIVE WORKLOAD

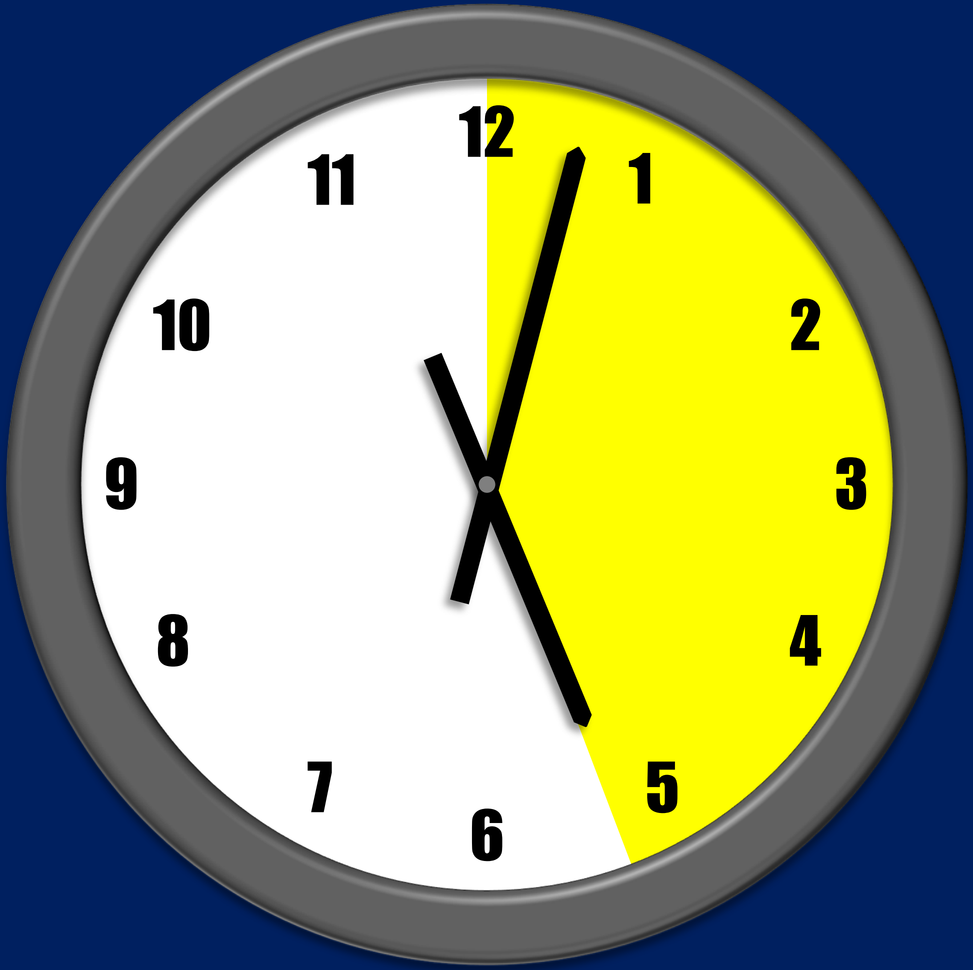
	Mental					
Physical	.479*	Physical				
Time	.547*	.541*	Time			
Performance	-.034	-.012	-.022	Performance		
Effort	.686*	.486*	.509*	-.009	Effort	
Frustration	.468*	.334*	.429*	-.315*	.469*	Frustration

* p < .001

FATIGUE & FRUSTRATION

	Mental	Physical	Time	Performance	Effort	Frustration
∆Fatigue	.263*	.225*	.162*	-.078	.227*	.173*
∆Frustration	.238*	.194*	.201*	-.184*	.277*	

* $p < .01$


12
1
2
3
4
5
6
7
8
9
10
11

OPERATION LENGTH

	Mental	Physical	Time	Performance	Effort	Frustration
Operation Length	.376*	.253*	.271*	.032	.296*	.176*

* p < .001

OPERATION LENGTH

	ΔFatigue	ΔFrustration
Operation Length	.361*	.210*

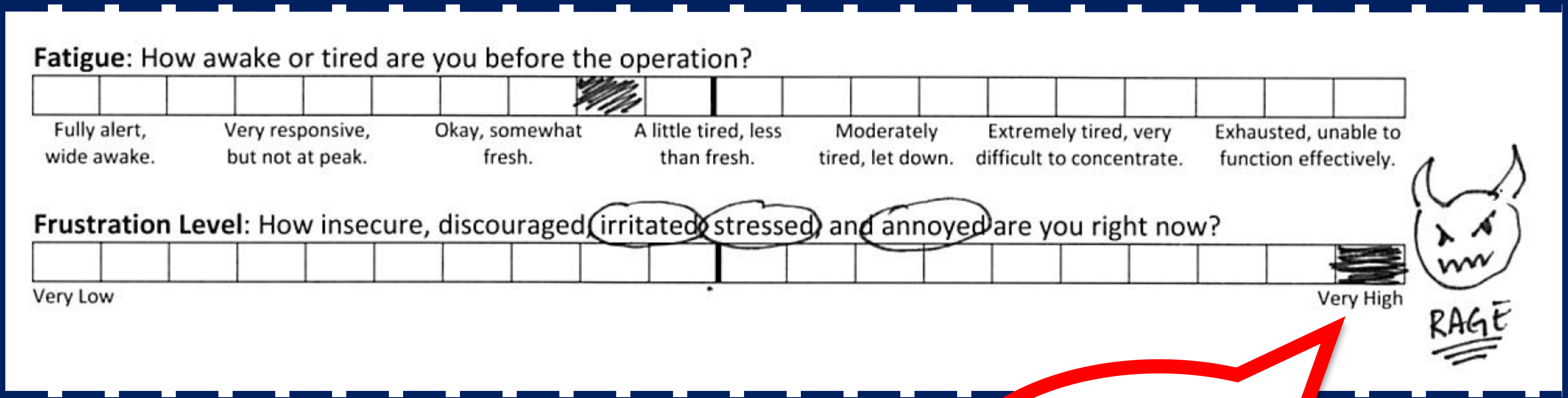
* $p < .001$

< 5 Hours Δ10% > 5 Hours

Failure is not an option.

Locus of control.

The extent to which a person feels that they have control over the outcome of events in their lives.



Fatigue: How awake or tired are you before the operation?

								▨											

Fully alert, wide awake. — Very responsive, but not at peak. — Okay, somewhat fresh. — A little tired, less than fresh. — Moderately tired, let down. — Extremely tired, very difficult to concentrate. — Exhausted, unable to function effectively.

Frustration Level: How insecure, discouraged, [✓ irritated], [✓ stressed], and [✓ annoyed] are you right now?

																			▨

Very Low — Very High

RAGE

Significantly dropped after the operation!

SUMMARY

Tactical cyber operations increase fatigue, frustration, and cognitive work

Longer operations are more tiring, frustrating, and mentally demanding

Fatigue and frustration begin to compound after 5 hours

However, operators always pull through with performance, but at what cost?

TAKEAWAYS

Use the Cyber Operations Stress Survey to evaluate your own operations

Review policies on breaks, scheduling, and operation length

Empower operators with happy, healthy work environments

Understanding Operator Fatigue, Frustration, and Cognitive Workload in Tactical Cybersecurity Operations

CL Paul and J Dykstra

Research Directorate
National Security Agency, U.S.A.

***Abstract:** While the human factors of mission critical systems such as air traffic control and weapons systems have been extensively studied, there has been little work on cyber operations. As with any system, the perfect storm of complex tasks in a high-risk environment takes an incredible toll on human operators, leading to errors, decreased performance, and burnout. An extensive study of tactical cyber operations at the National Security Agency found that operator fatigue, frustration, and cognitive workload significantly increase over the course of an operation. A discussion of these findings helps us understand the impact that the high-stress, high-risk environment of tactical cyber operations has on its operators.*

Keywords: *Cyber Operations, Cognitive Workload, Fatigue, Frustration, Burnout, Human Factors, Cybersecurity*

Introduction

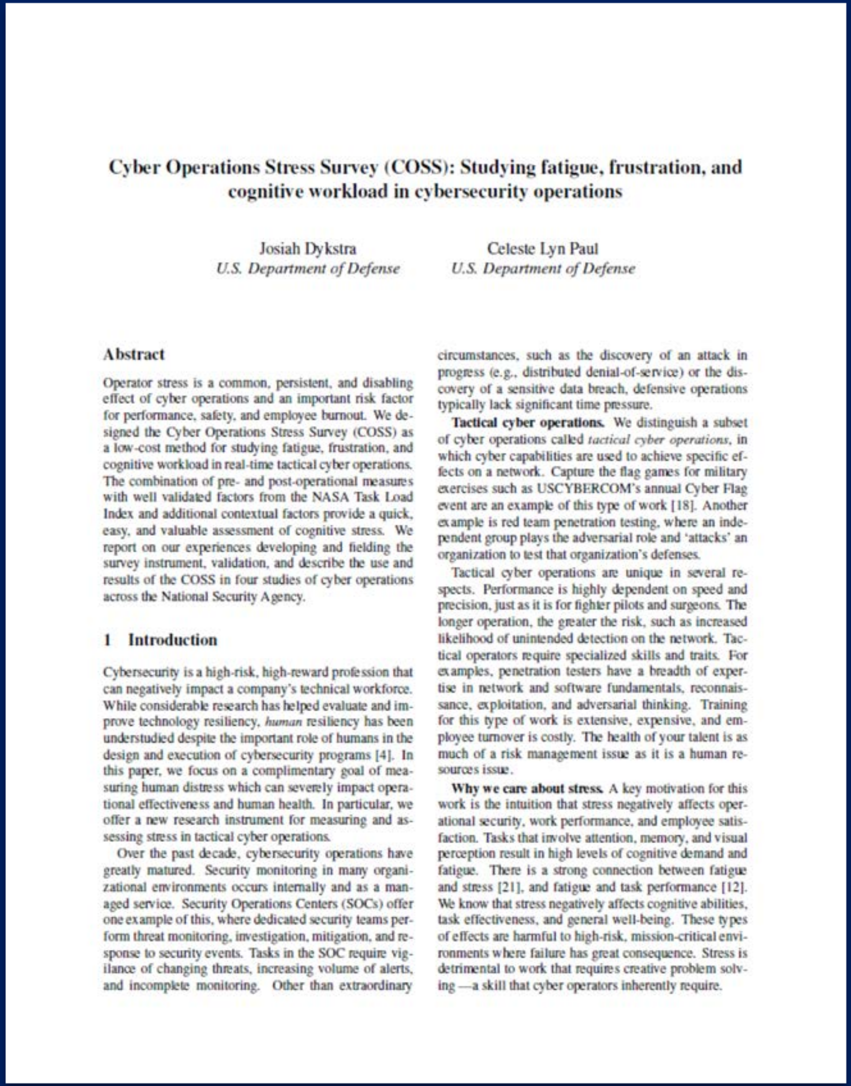
Cybersecurity operations are a mission-critical service for the safety and business continuity of companies and organizations in the digital world. From red team network penetration testing to real-time defensive monitoring, evolving technology and threats to the network make cybersecurity operations high-value, complex, and difficult. This environment is considerably high-risk, and success or failure can greatly affect the mission or reputation of an organization. Research and development for cybersecurity operations has heavily focused on technological means of achieving a more secure enterprise. However, it is the human experts who play the most critical role in the deployment, configuration, monitoring, and operation of networks.

The National Security Agency (NSA) coordinates, directs, and performs highly specialized activities to protect U.S. government information systems and to produce foreign signals intelligence. One of NSA's missions is to defend the Department of Defense Information Network (DODIN), National Security Systems (NSS), and other critical U.S. government systems. Intelligence analysts and network operators work together around the clock to detect, assess, and prevent foreign threats to networks. In addition to its headquarters in Maryland, NSA has cryptologic centers in Colorado, Georgia, Hawaii, and Texas that also conduct foreign signals intelligence, cyberspace operations, and information assurance operations.

NSA recruits and hires computer network operators to both defend U.S. military networks and to exploit the networks of foreign adversaries. For these jobs, NSA seeks people with

Journal of Information Warfare (2017) 16.2: 1-11 1
ISSN 1445-3312 Print/ISSN 1445-3347 Online

Journal of Information Warfare (2017).
https://www.jinfowar.com/journal/volume-16-issue-2/understanding-operator-fatigue-frustration-cognitive-workload-tactical-cybersecurity-operations



Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations

Josiah Dykstra
U.S. Department of Defense

Celeste Lyn Paul
U.S. Department of Defense

Abstract

Operator stress is a common, persistent, and disabling effect of cyber operations and an important risk factor for performance, safety, and employee burnout. We designed the Cyber Operations Stress Survey (COSS) as a low-cost method for studying fatigue, frustration, and cognitive workload in real-time tactical cyber operations. The combination of pre- and post-operational measures with well validated factors from the NASA Task Load Index and additional contextual factors provide a quick, easy, and valuable assessment of cognitive stress. We report on our experiences developing and fielding the survey instrument, validation, and describe the use and results of the COSS in four studies of cyber operations across the National Security Agency.

1 Introduction

Cybersecurity is a high-risk, high-reward profession that can negatively impact a company's technical workforce. While considerable research has helped evaluate and improve technology resiliency, *human* resiliency has been understudied despite the important role of humans in the design and execution of cybersecurity programs [4]. In this paper, we focus on a complimentary goal of measuring human distress which can severely impact operational effectiveness and human health. In particular, we offer a new research instrument for measuring and assessing stress in tactical cyber operations.

Over the past decade, cybersecurity operations have greatly matured. Security monitoring in many organizational environments occurs internally and as a managed service. Security Operations Centers (SOCs) offer one example of this, where dedicated security teams perform threat monitoring, investigation, mitigation, and response to security events. Tasks in the SOC require vigilance of changing threats, increasing volume of alerts, and incomplete monitoring. Other than extraordinary circumstances, such as the discovery of an attack in progress (e.g., distributed denial-of-service) or the discovery of a sensitive data breach, defensive operations typically lack significant time pressure.

Tactical cyber operations. We distinguish a subset of cyber operations called *tactical cyber operations*, in which cyber capabilities are used to achieve specific effects on a network. Capture the flag games for military exercises such as USCYBERCOM's annual Cyber Flag event are an example of this type of work [18]. Another example is red team penetration testing, where an independent group plays the adversarial role and 'attacks' an organization to test that organization's defenses.

Tactical cyber operations are unique in several respects. Performance is highly dependent on speed and precision, just as it is for fighter pilots and surgeons. The longer operation, the greater the risk, such as increased likelihood of unintended detection on the network. Tactical operators require specialized skills and traits. For examples, penetration testers have a breadth of expertise in network and software fundamentals, reconnaissance, exploitation, and adversarial thinking. Training for this type of work is extensive, expensive, and employee turnover is costly. The health of your talent is as much of a risk management issue as it is a human resources issue.

Why we care about stress. A key motivation for this work is the intuition that stress negatively affects operational security, work performance, and employee satisfaction. Tasks that involve attention, memory, and visual perception result in high levels of cognitive demand and fatigue. There is a strong connection between fatigue and stress [21], and fatigue and task performance [12]. We know that stress negatively affects cognitive abilities, task effectiveness, and general well-being. These types of effects are harmful to high-risk, mission-critical environments where failure has great consequence. Stress is detrimental to work that requires creative problem solving —a skill that cyber operators inherently require.

Cyber Security Experimentation and Test (2018).
https://www.usenix.org/conference/cset18/presentation/dykstra

STRESS & HACKING

Understanding Cognitive Stress in Tactical Cyber Operations

For more information contact:

NSA PUBLIC AFFAIRS OFFICE
mediarelations@nsa.gov
+1 (301) 688-6311