CAN MUGGLES DO MAGIC?

MALWARE ANALYSIS FOR POLICY PEOPLE

Hello

my name is

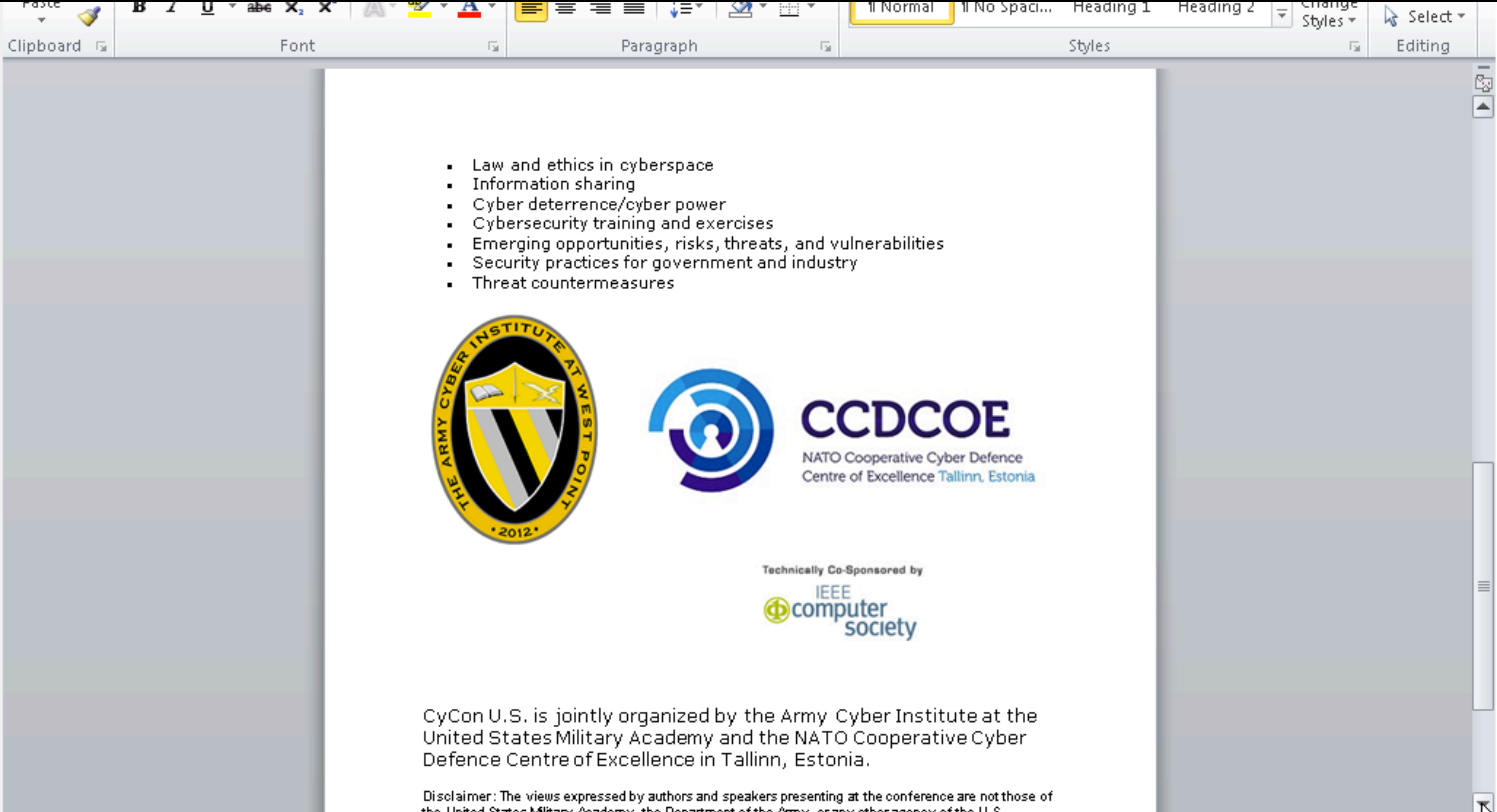
Mara

Washington, DC

OBSERVED IN THE WILD

CyCon U.S.
International Conference on Cyber Conflict
THE ARMY CYBER INSTITUTE AT WEST POINT
2012
CCDCOE
NATO Cooperative Cybe
Tallinn, Esto
CyCon

MALWARE IMITATES LIFE


Paste
Clipboard
Font
Paragraph
¶ Normal
¶ No Spaci...
Heading 1
Heading 2
Change Styles
Styles
Select
Editing
THE ARMY CYBER INSTITUTE AT WEST POINT
2012
CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Technically Co-Sponsored by
IEEE computer society

- Law and ethics in cyberspace
- Information sharing
- Cyber deterrence/cyber power
- Cybersecurity training and exercises
- Emerging opportunities, risks, threats, and vulnerabilities
- Security practices for government and industry
- Threat countermeasures

CyCon U.S. is jointly organized by the Army Cyber Institute at the United States Military Academy and the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.

Disclaimer: The views expressed by authors and speakers presenting at the conference are not those of the United States Military Academy, the Department of the Army, or any other agency of the U.S.

> "All offensive problems are technical problems, and all defensive problems are political problems."

– THOMAS DULLIEN [HALVAR FLAKE], BLACKHAT ASIA 2017.

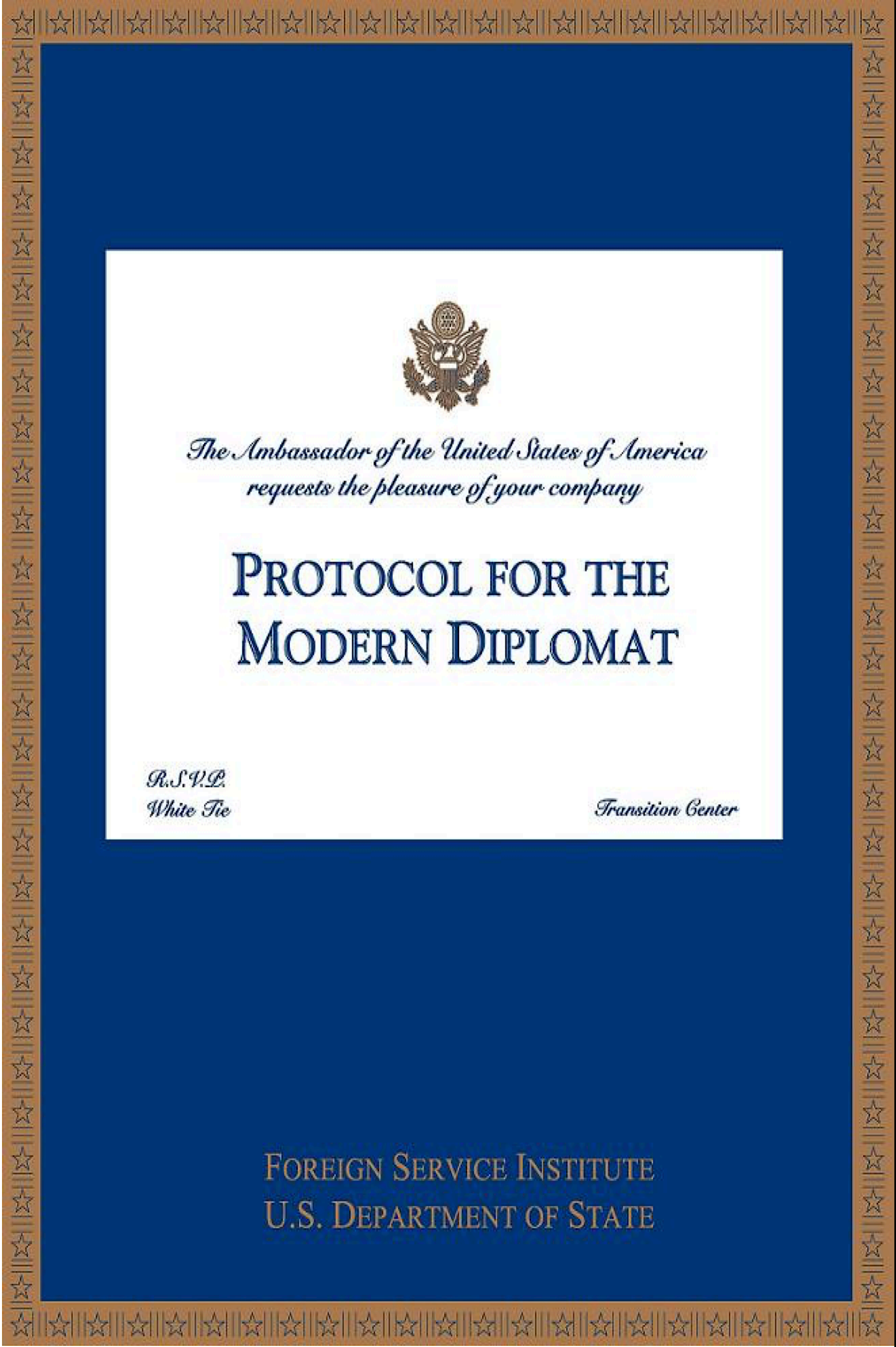
BAD IDEAS IN CYBER POLICY

A BRIEF HISTORY

- Export controls (cryptography, “intrusion software”)
- ‘Hacking back,’ a.k.a. cyber letters of marque and reprisal, a.k.a. cyber privateers
- Cyber-as-armed-conflict <= really, *really* terrible idea

POLICY

HOW DOES IT WORK?



The Ambassador of the United States of America
requests the pleasure of your company

PROTOCOL FOR THE
MODERN DIPLOMAT

R.S.V.P.
White Tie

Transition Center

FOREIGN SERVICE INSTITUTE
U.S. DEPARTMENT OF STATE

- Démarche (strongly-worded letter)
- Economic penalties (i.e. trade)
- Targeted sanctions (e.g. against individuals or entities)

CURRENT STATE OF 'CYBER' DOCTRINE

GAPING ABYSS

WHY DOESN'T THIS WORK?

- Open-source / industry analysis is fragmented
- Analysis lacks rigour
- Confidence is 100 or 0
- Weak third-party attribution

- Group 74 TALOS
- APT28 MANDIANT®
- Sofacy paloalto NETWORKS®
- Fancy Bear CROWDSTRIKE
- Tsar Team eset®
- Pawn Storm iSIGHTPARTNERS
- Sednit TREND MICRO
- GRIZZLY STEPPE (APT28 + APT29) U.S. DEPARTMENT OF HOMELAND SECURITY

- Group 74 Talos
- APT28 MANDIANT
- Sofacy paloalto NETWORKS
- Fancy Bear CROWDSTRIKE
- Tsar Team eset
- Pawn Storm iSIGHTPARTNERS
- Sednit TREND MICRO
- GRIZZLY STEPPE (APT28 + APT29) U.S. DEPARTMENT OF HOMELAND SECURITY

"The technology is only interesting insofar as it answers policy questions."

–JEFFREY LEWIS (@ARMSCONTROLWONK)

INTERESTING STUFF

- Attribution : let’s talk about confidence
    - Verification in arms control is a mosaic of imperfect technical indicators whose strengths + limits are generally agreed
- Intent : what can we infer from design?
    - What does it mean when anatomically correct ransomware is observed to function as a wiper?
    - Modularity / ease of code re-use *super* interesting

MOAR INTERESTING STUFF

- [your thoughts here]

CONTACT

- @marasawr open dms
- marasawr [at] gmail
- linkedin.com/in/marasawr