

VULNERABILITIES AND THEIR SURROUNDING ETHICAL QUESTIONS:

WHAT THE PRIVATE SECTOR CAN DO

Alfonso De Gregorio, Zeronomicon

**EU Zero-day Vulnerability Management Workshop 2017
January 27, Brussels**



Discuss

@ZERONOMICON

#VULNETHICS



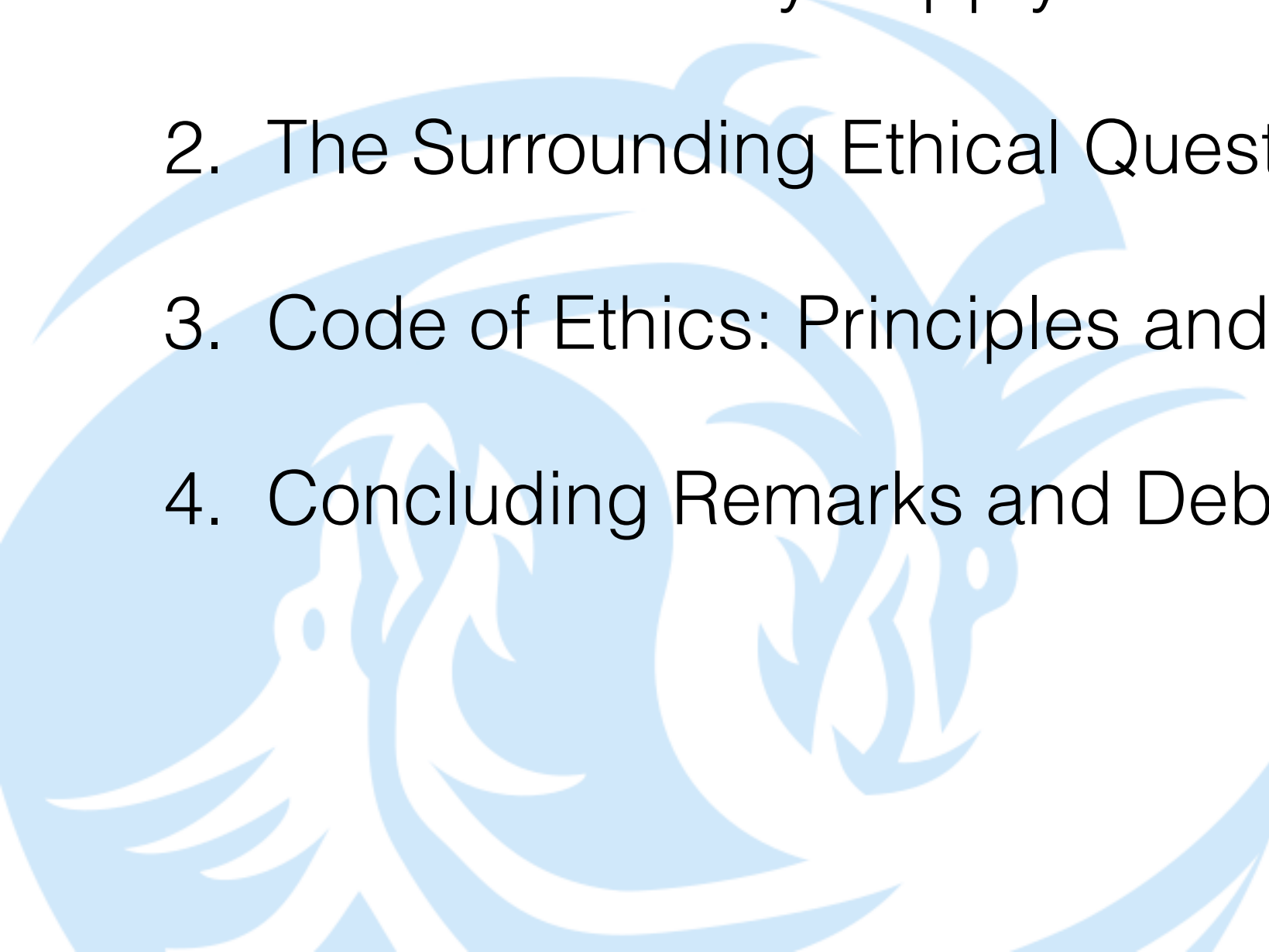
Discuss

@ZERONOMICON

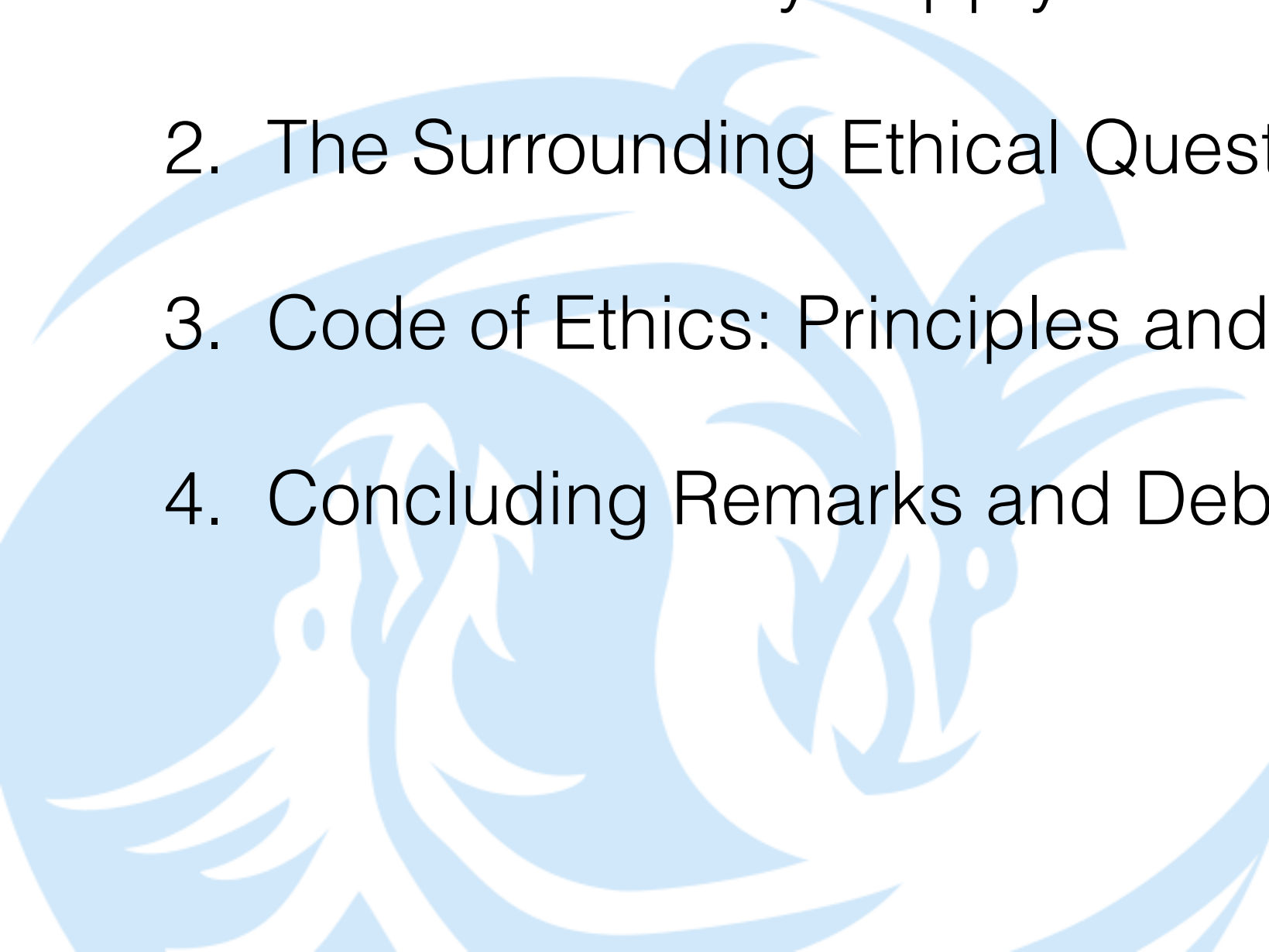
#VULNETHICS



Agenda

1. The Vulnerability Supply Chain
 2. The Surrounding Ethical Questions
 3. Code of Ethics: Principles and Standards
 4. Concluding Remarks and Debate
- 

Agenda

1. The Vulnerability Supply Chain
 2. The Surrounding Ethical Questions
 3. Code of Ethics: Principles and Standards
 4. Concluding Remarks and Debate
- 

THE VULNERABILITIES

SUPPLY CHAIN









VULNERABILITIES ARE LIKE POLLUTANTS







UNRESTRAINED **VULNERABILITY DUMPING**



IMPORTANT NO
UNTREATED WATER
SEWAGE DO NOT
DRINK OR SWIM







Policy



UNRESTRAINED
VULNERABILITY DUMPING



IMPORTANT NO
UNTREATED WATER
SEWAGE DO NOT
DRINK OR SWIM











PERVERSE INCENTIVE





**“patching allows software manufacturers
to optimize market and legal
protections by “re-negotiating” contract
terms buyers could not
negotiate in the first place”**

– David Rice

iPhone Software Update

Safety Info: Read Important Product Information Guide before use: www.apple.com/support/manuals/iphone

ENGLISH

IMPORTANT: BY USING YOUR iPhone, iPad OR iPod touch ("iOS Device"), YOU ARE AGREEING TO BE BOUND BY THE FOLLOWING TERMS:

- A. APPLE iOS SOFTWARE LICENSE AGREEMENT**
- B. NOTICES FROM APPLE**

APPLE INC.
iOS SOFTWARE LICENSE AGREEMENT
Single Use License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING YOUR iOS DEVICE OR DOWNLOADING THE SOFTWARE UPDATE ACCOMPANYING THIS LICENSE. BY USING YOUR iOS DEVICE OR DOWNLOADING A SOFTWARE UPDATE, AS APPLICABLE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE iOS DEVICE OR DOWNLOAD THE SOFTWARE UPDATE.

IF YOU HAVE RECENTLY PURCHASED AN iOS DEVICE AND YOU DO NOT AGREE TO THE TERMS OF THE LICENSE, YOU MAY RETURN THE iOS DEVICE WITHIN THE RETURN PERIOD TO THE APPLE STORE OR AUTHORIZED DISTRIBUTOR WHERE YOU OBTAINED IT FOR A REFUND, SUBJECT TO APPLE'S RETURN POLICY FOUND AT http://www.apple.com/legal/sales_policies/.

1. General.

(a) The software (including Boot ROM code, embedded software and third party software), documentation, interfaces, content, fonts and any data that came with your iOS Device ("Original iOS Software"), as may be updated or replaced by

Save

Decline

Agree



MADE IN CCCP // WWW.MICCCP.COM





好吃滷味

超大大雞排

大腸包小腸

肉燥麵
花枝凍麵

豬血糕

香炸臭豆腐

麻辣涼麵

香酥



**VULNERABILITIES ARE
THE UNKNOWN CURRENCY
OF THE SECURITY AFTERMARKET**

A faint, light blue watermark of a tiger's head is visible in the background, positioned behind the text. The tiger is facing right, with its mouth slightly open, showing its teeth. The watermark is semi-transparent and covers the lower half of the image.



THE SURROUNDING ETHICAL QUESTIONS



из манежа







WRONG

RIGHT

?

RIGHT

?

WRONG

WRONG

RIGHT

?

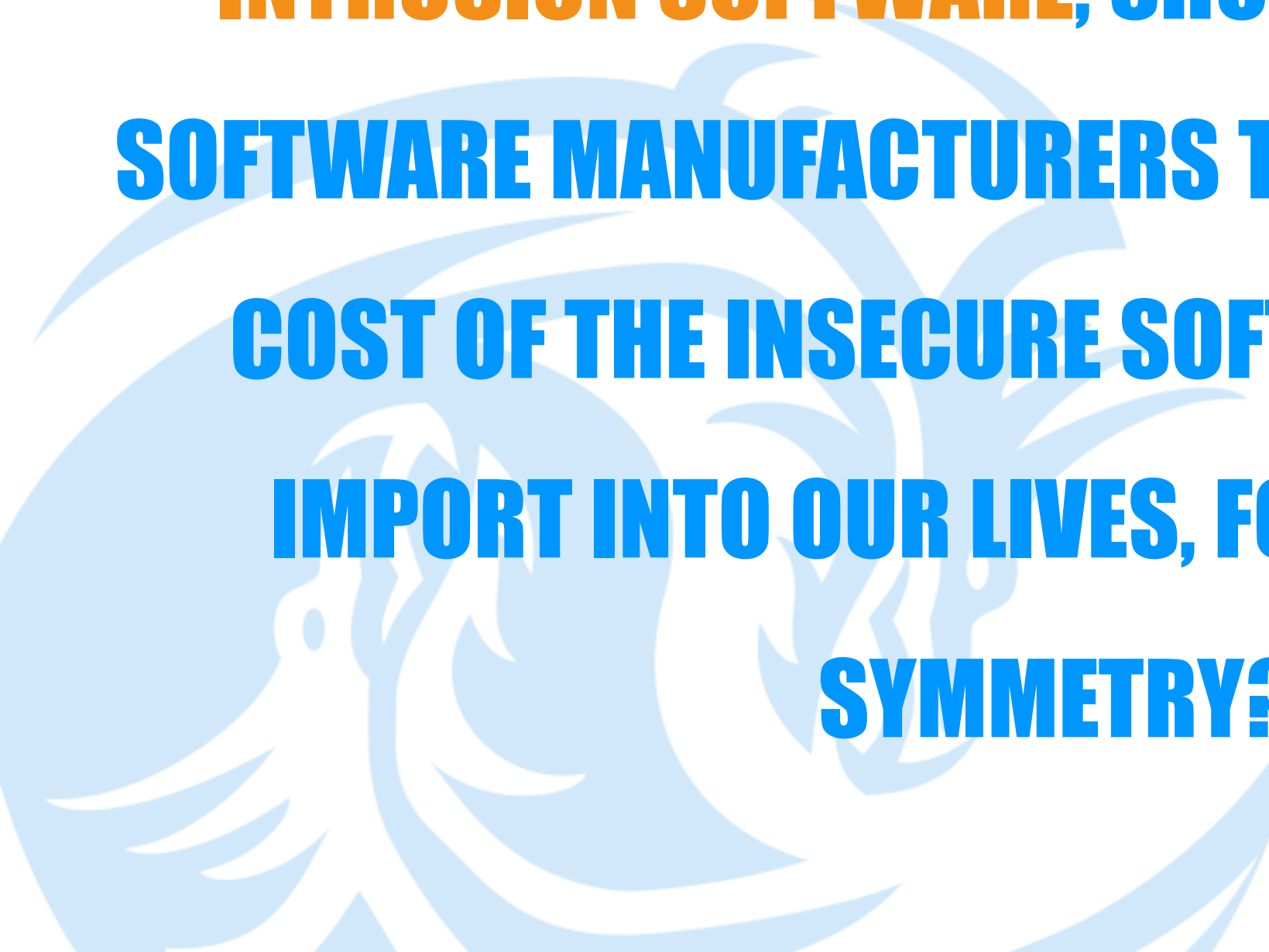
WHO HOLDS
THE MORAL LOW GROUND?



**WHO ARE THE ONES
THAT EXPLOIT US THE MOST?**



**IF OUR GOVERNMENTS INTRODUCE TRADE
CONTROLS TO ADMINISTER THE EXPORT OF
INTRUSION SOFTWARE, SHOULD WE DEMAND
SOFTWARE MANUFACTURERS TO INTERNALISE THE
COST OF THE INSECURE SOFTWARE THAT WE
IMPORT INTO OUR LIVES, FOR REASONS OF
SYMMETRY?**



**SHOULD WE MAKE THEM LIABLE FOR THE DEFECTS
AND FLAWS THAT ALLOW THE INTRUSION IN THE
FIRST PLACE?**



**WITH INCOMPLETE KNOWLEDGE ABOUT THE REAL-
WORLD SECURITY OF SYSTEMS WE ENTRUST OUR
BUSINESS, IS IT ETHICAL TO REFRAIN US FROM
HUNTING VULNERABILITIES OR PREVENT OTHERS
FROM DOING LIKEWISE?**

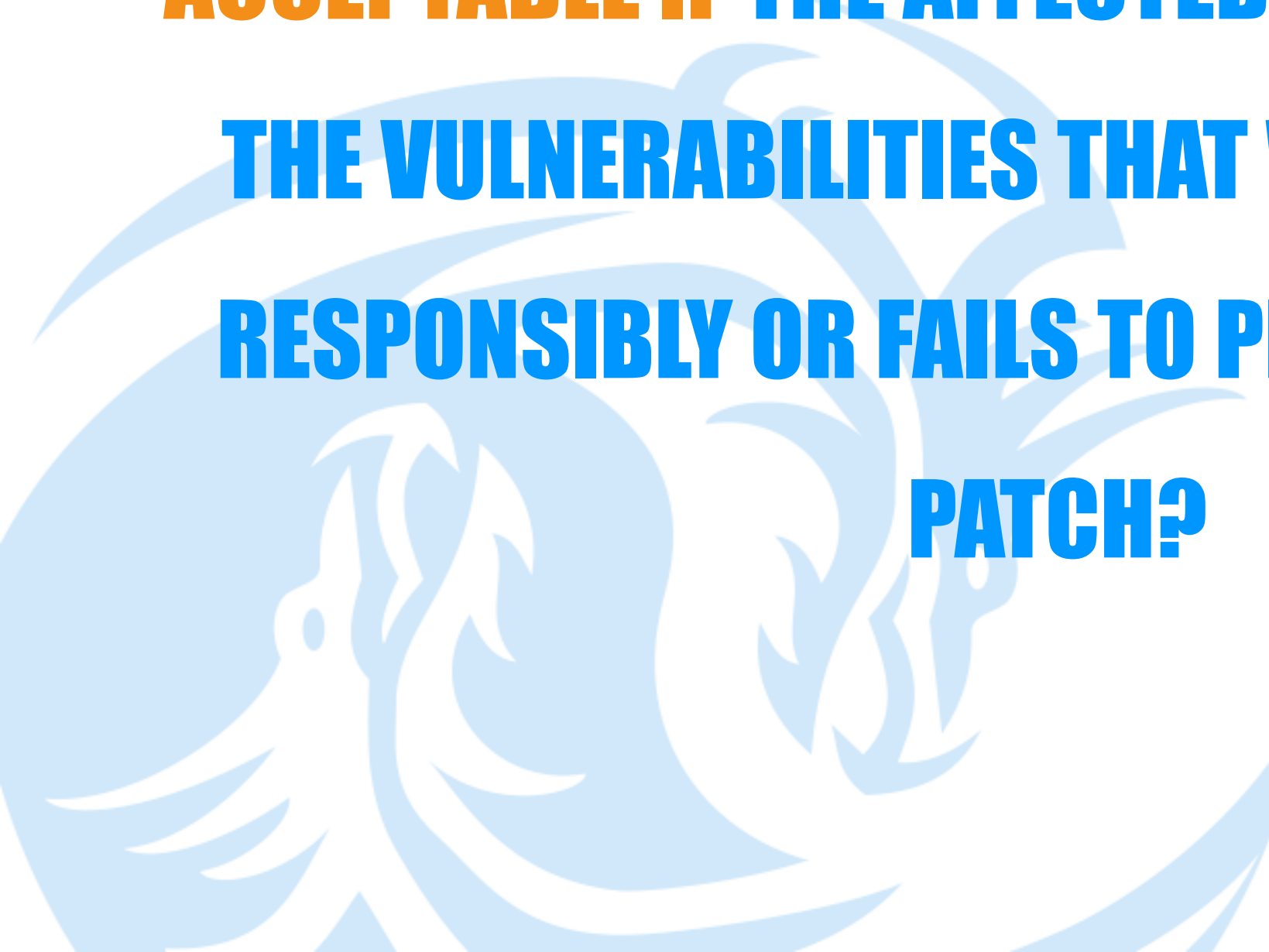
**AND, WHAT SHOULD DO A SECURITY RESEARCHER
WITH THE VULNERABILITIES WHEN THEY GET
FOUND?**



**IS FULL DISCLOSURE AN ACCEPTABLE COURSE OF
ACTION?**



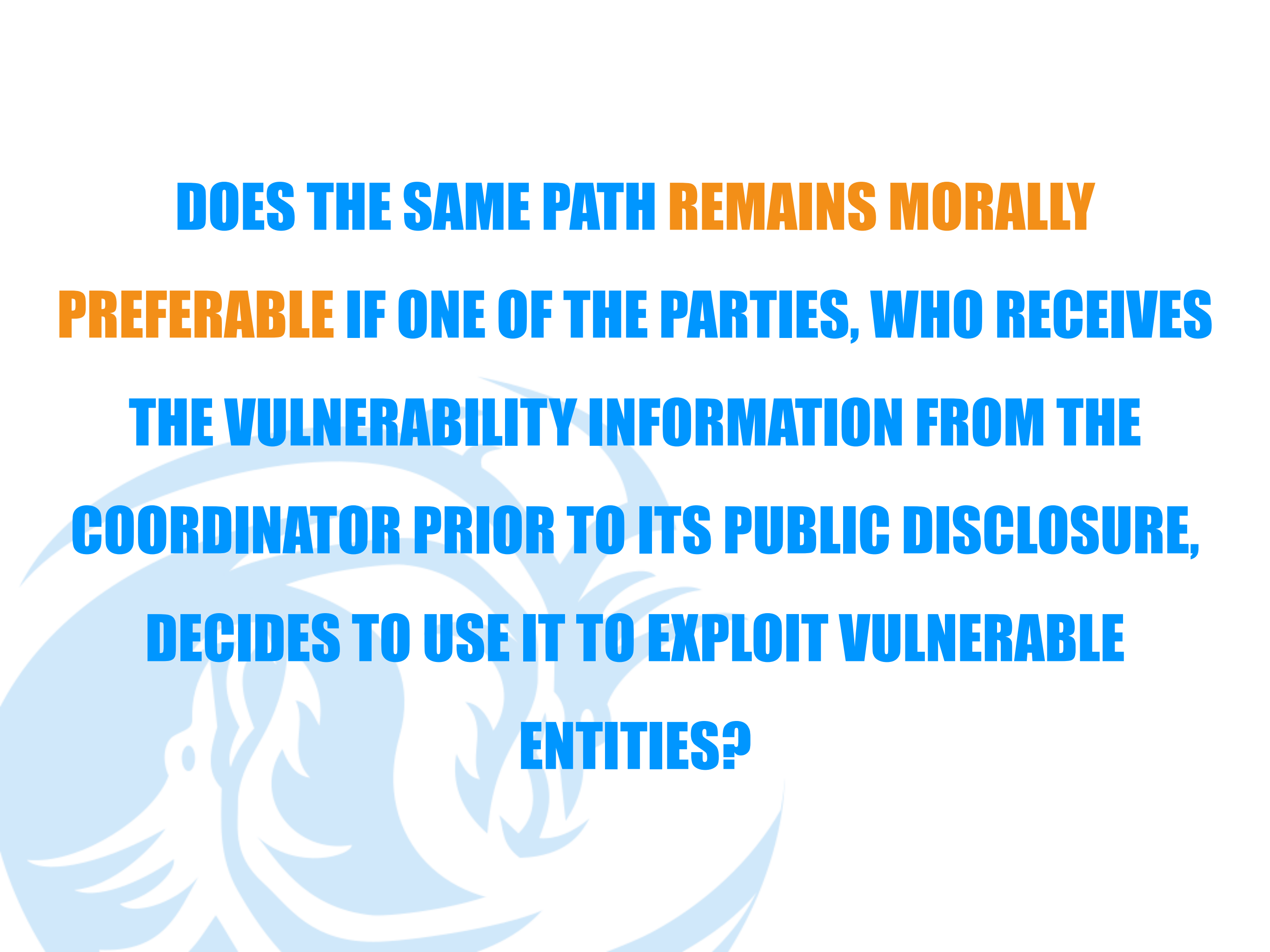
**DOES FULL DISCLOSURE BECOMES MORE
ACCEPTABLE IF THE AFFECTED VENDOR IGNORES
THE VULNERABILITIES THAT WERE REPORTED
RESPONSIBLY OR FAILS TO PROVIDE A TIMELY
PATCH?**



**DOES COORDINATED VULNERABILITY DISCLOSURE
PROVIDE A MORE ETHICALLY SOUND PATH TO BE
TAKEN?**



**DOES THE SAME PATH REMAINS MORALLY
PREFERABLE IF ONE OF THE PARTIES, WHO RECEIVES
THE VULNERABILITY INFORMATION FROM THE
COORDINATOR PRIOR TO ITS PUBLIC DISCLOSURE,
DECIDES TO USE IT TO EXPLOIT VULNERABLE
ENTITIES?**



**ARE BUG BOUNTY PROGRAMS EXPLOITING BOUNTY
HUNTERS?**



SHOULD BUG HUNTERS **PRETEND TO GET PAID IF
THE OTHER PARTY HAS NOT ASKED THEM TO DO
THEIR WORK?**

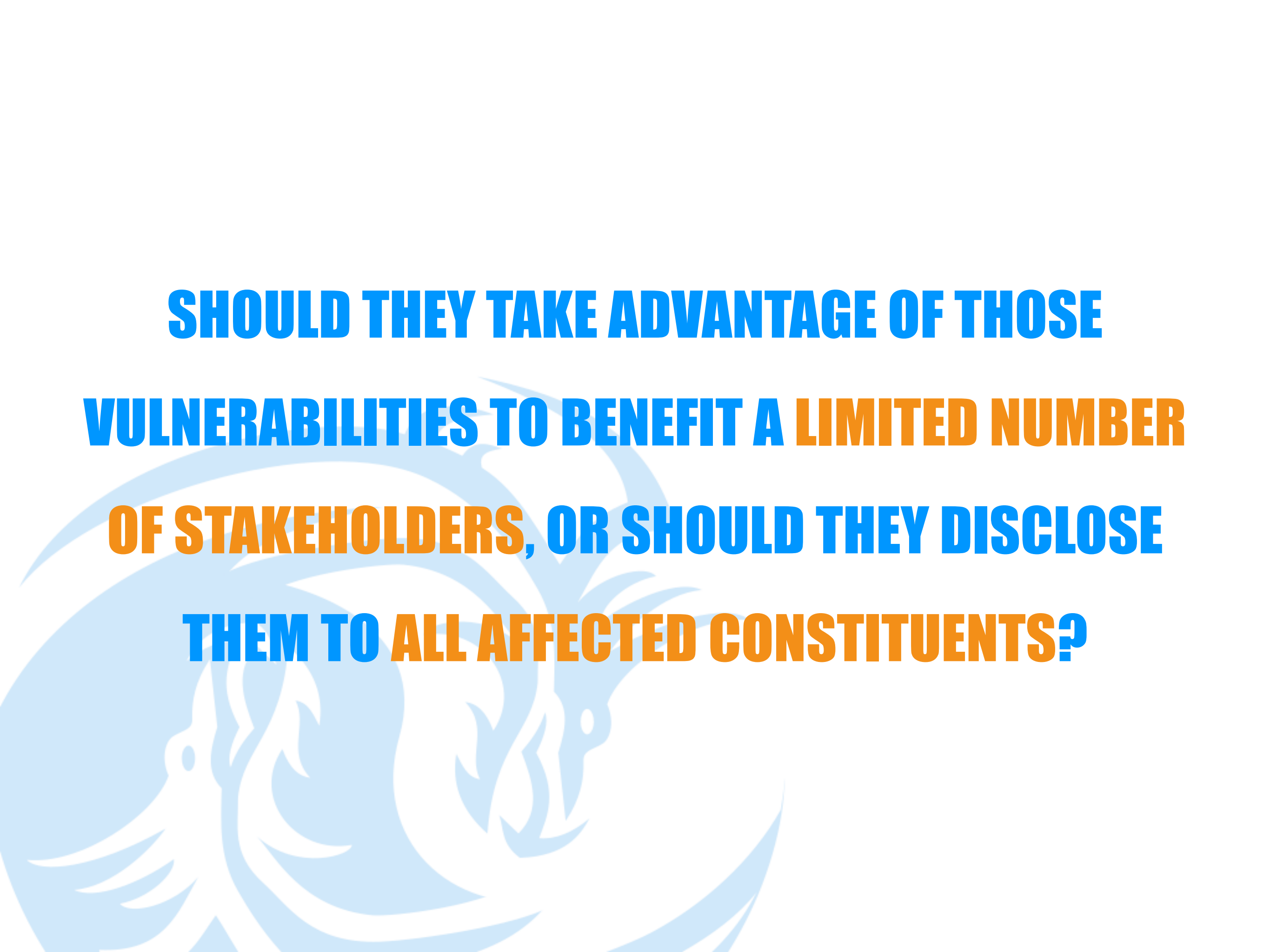




**WHAT GOVERNMENT SECURITY AGENCIES SHOULD
DO WITH VULNERABILITIES?**

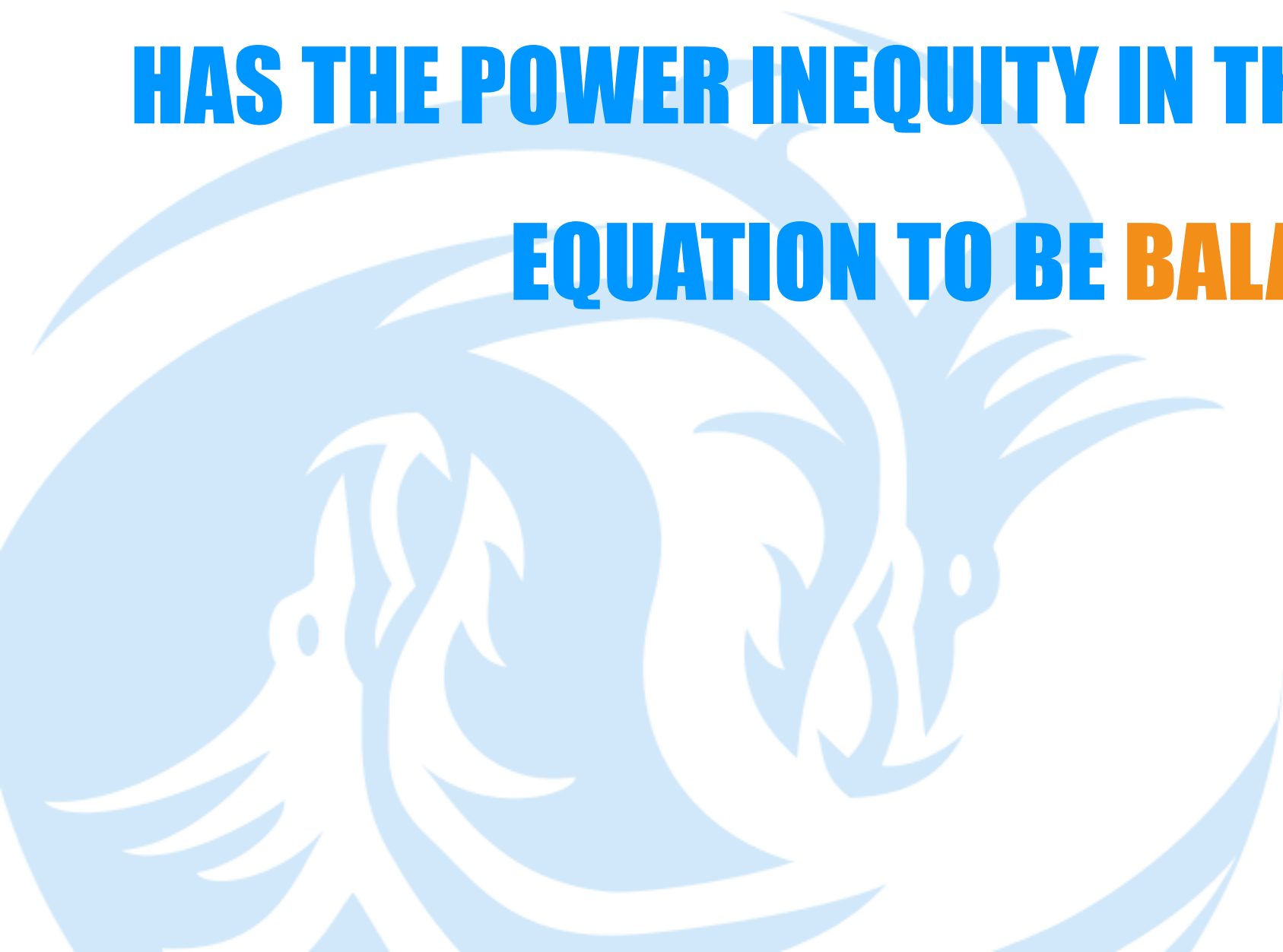
**SHOULD THEY EXPLOIT THEM OR SHOULD THEY LET
EVERYBODY ELSE MITIGATE THEM, IN THE WAY THEY
ALREADY DO?**





**SHOULD THEY TAKE ADVANTAGE OF THOSE
VULNERABILITIES TO BENEFIT A LIMITED NUMBER
OF STAKEHOLDERS, OR SHOULD THEY DISCLOSE
THEM TO ALL AFFECTED CONSTITUENTS?**

**HAS THE POWER INEQUITY IN THE VULNERABILITY
EQUATION TO BE BALANCED?**



**WITH ENTITIES AFFECTED BY VULNERABILITIES
SPREAD ALL AROUND THE WORLD, HOW TO INFORM
THE PUBLIC?**



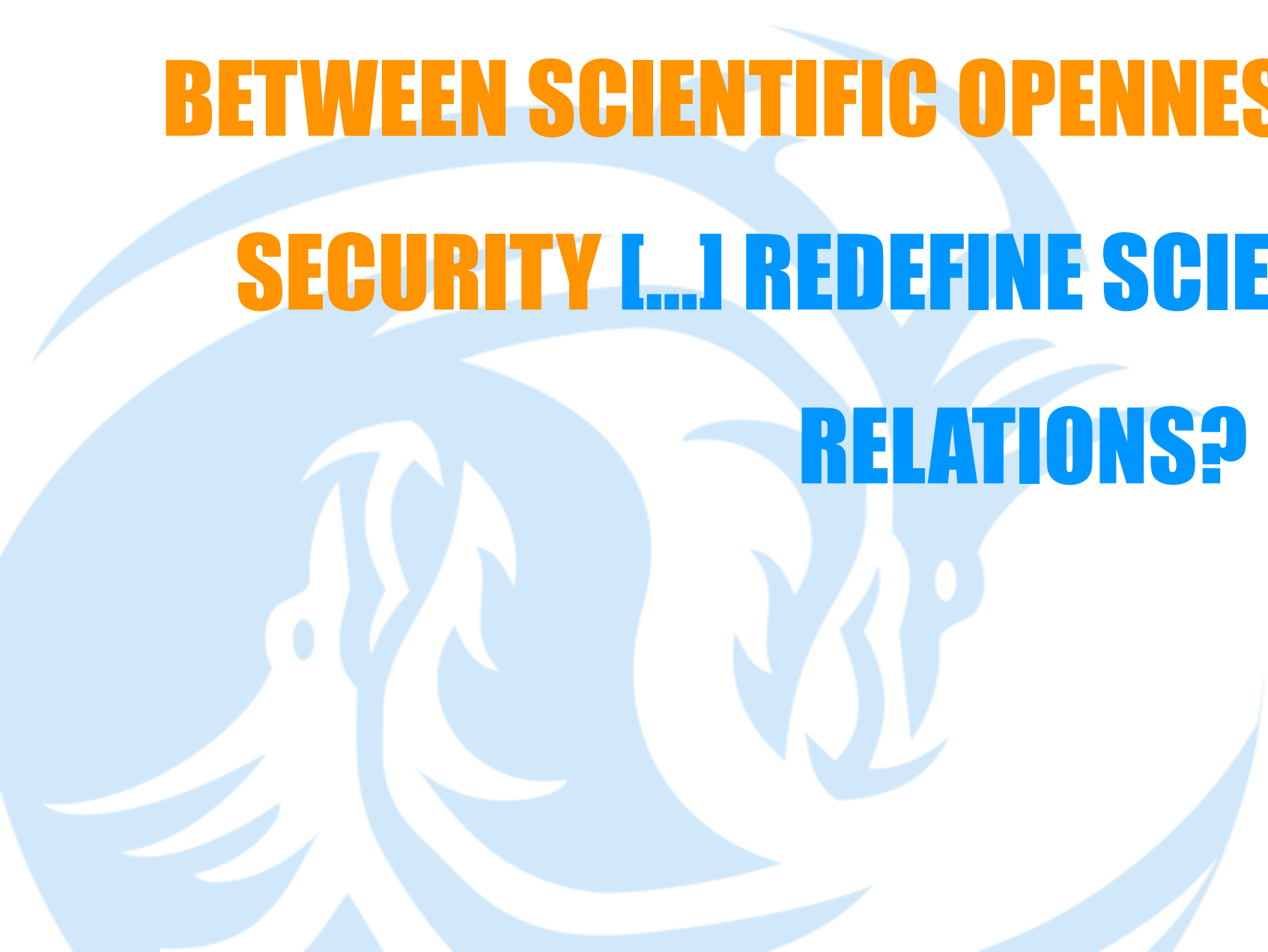
**WITH VENDORS THREATENING LEGAL ACTION AND
SUPPORTED BY THEIR SIGNIFICANT FINANCIAL
RESOURCES, HOW TO PROTECT THE SECURITY
RESEARCHERS?**





**WITH OUR SOCIETY GROWING MORE DATA
INTENSIVE, HOW TO OVERSEE NOT ONLY MATERIAL
AND TECHNOLOGY BUT ALSO KNOWLEDGE?**

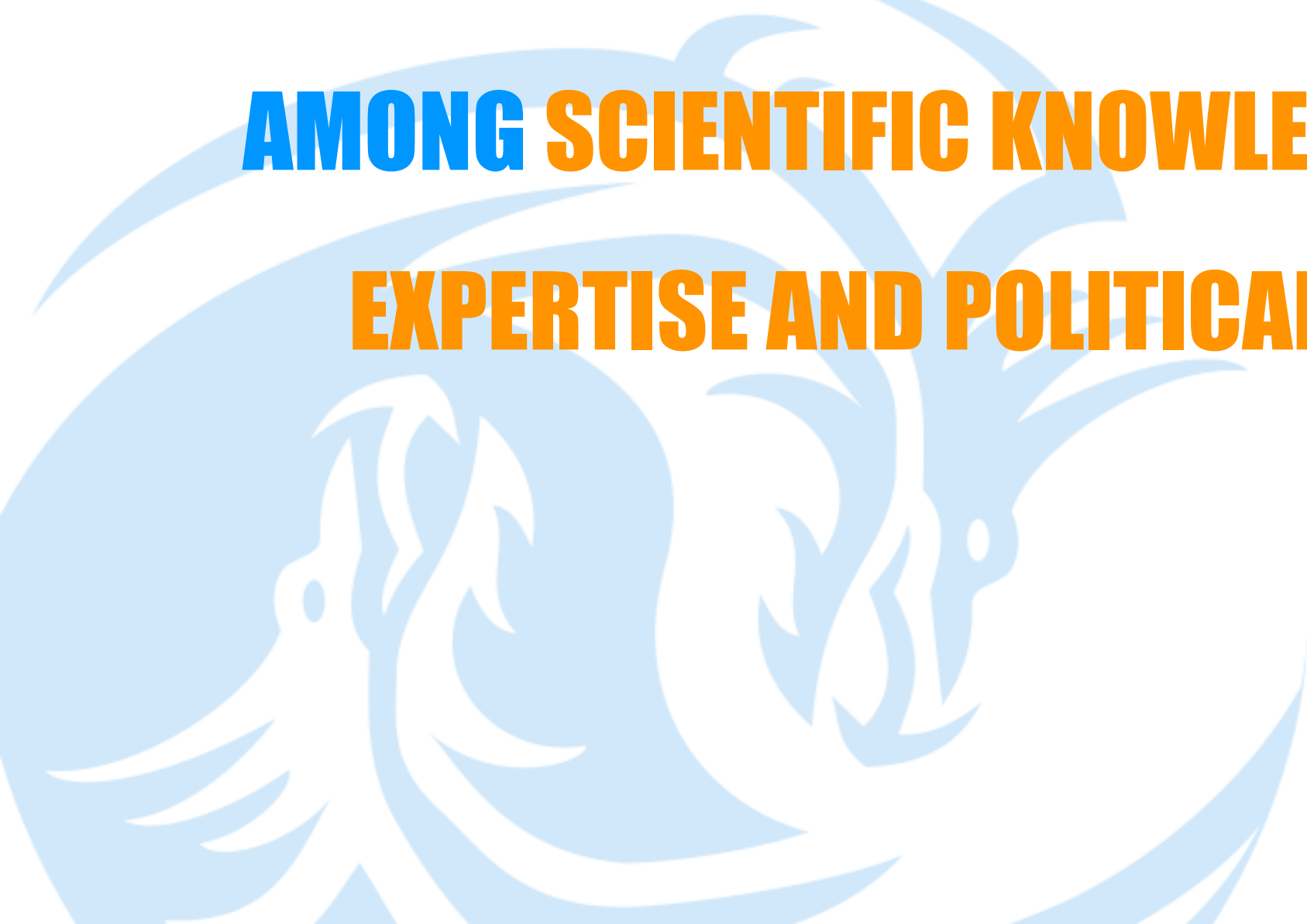
**HOW DO THE ATTEMPTS TO STRIKE A BALANCE
BETWEEN SCIENTIFIC OPENNESS AND NATIONAL
SECURITY [...] REDEFINE SCIENCE-SECURITY
RELATIONS?**





**HOW DOES SCIENTIFIC KNOWLEDGE BECOME
SUBJECT TO SECURITY GOVERNANCE?**

**HOW DOES THIS DYNAMIC AFFECT THE LINKS
AMONG SCIENTIFIC KNOWLEDGE, SECURITY
EXPERTISE AND POLITICAL DECISION?**



**CAN WE REGARD HACKING TO BE AN ETHICAL
PRACTICE AND CONDEMN, AT THE SAME TIME, THE
TRADE OF CAPABILITIES ENABLING THIS PRACTICE
AS IMMORAL?**



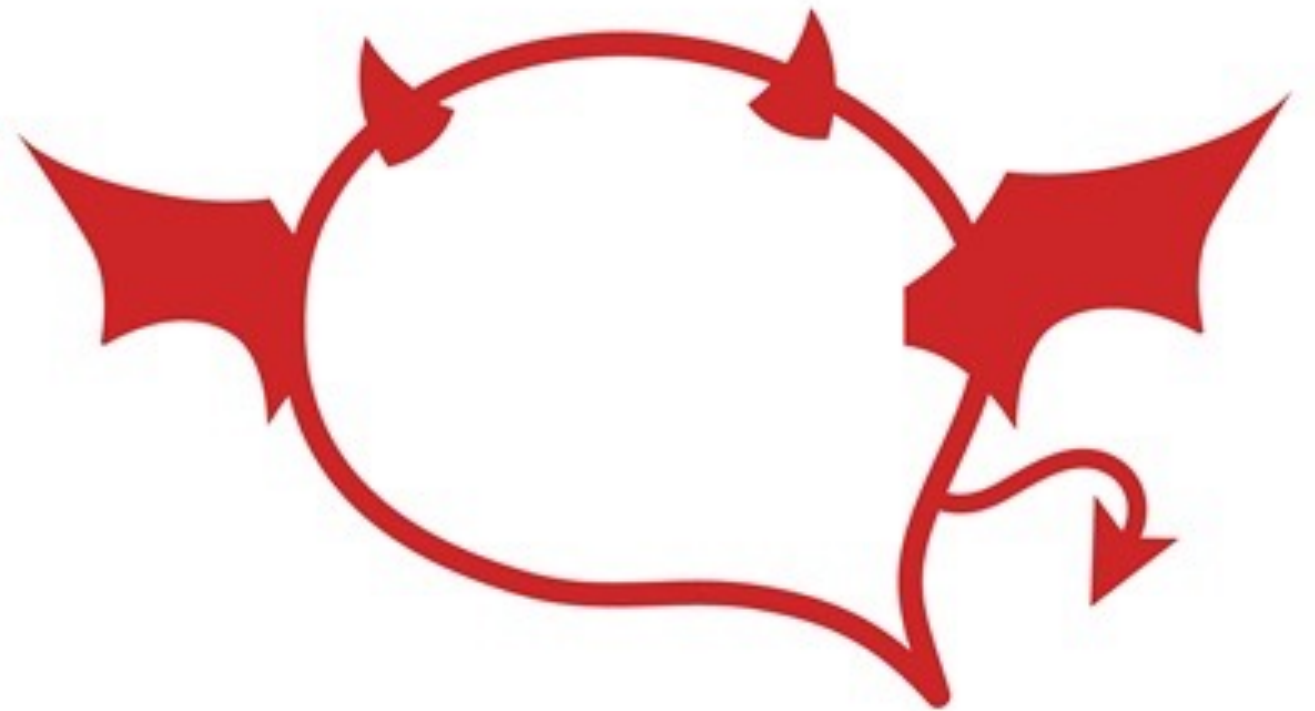


WHAT TO DO?

THE NON-ZERO SOCIETAL RISKS



NOT IPSO FACTO GOOD OR BAD



NOT IPSO FACTO GOOD OR BAD

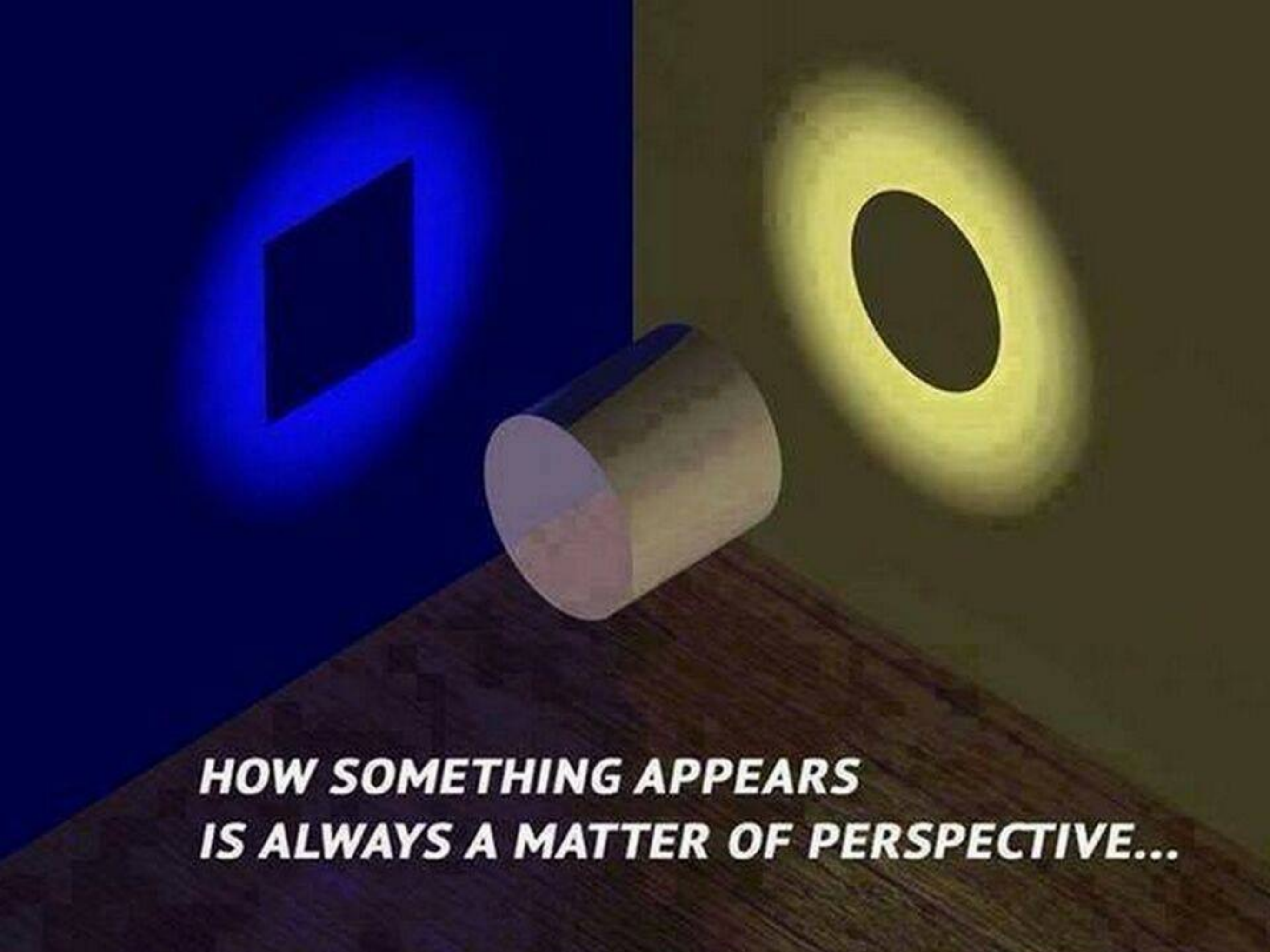


Network Attacks and Exploitation

A FRAMEWORK

Matthew Monte

WILEY



***HOW SOMETHING APPEARS
IS ALWAYS A MATTER OF PERSPECTIVE...***



Depending from which side of the playing field we look at things, the use of the same capability might be considered differently if it goes towards the creation or the detriment of









**ECONOMIC
ADVANTAGE**



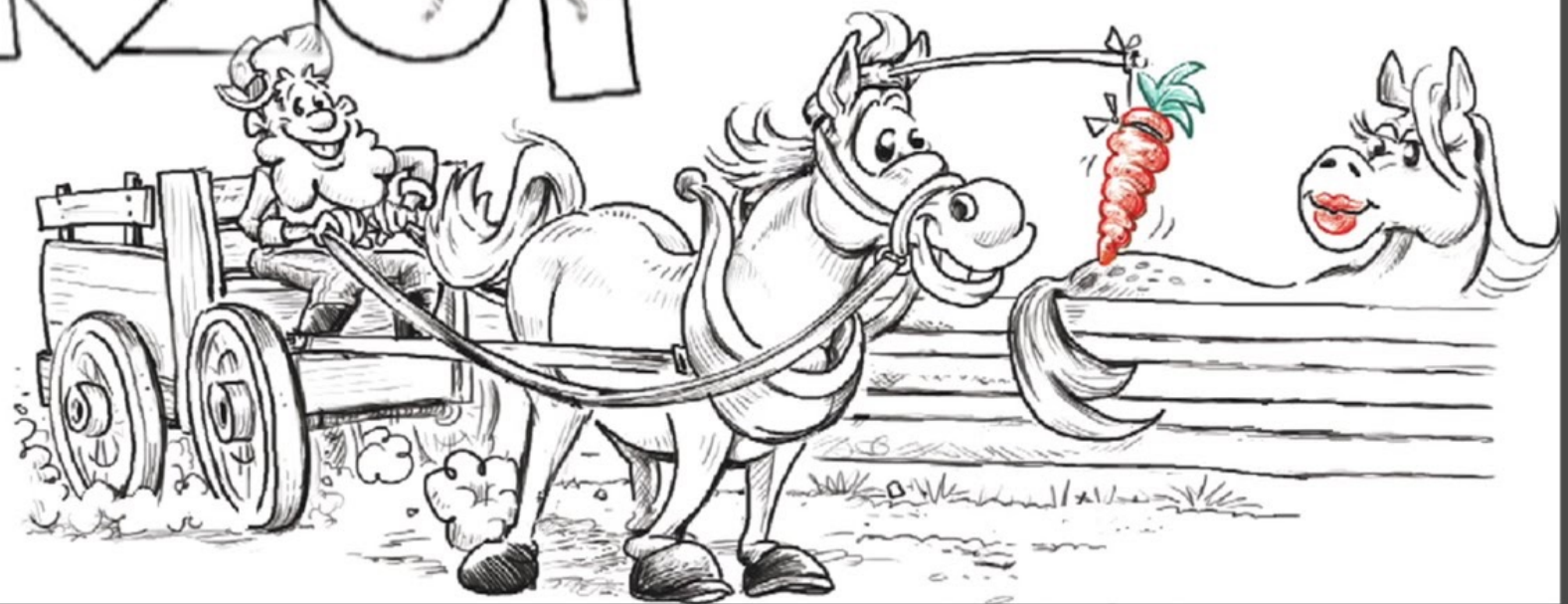








CONFLICT INTEREST

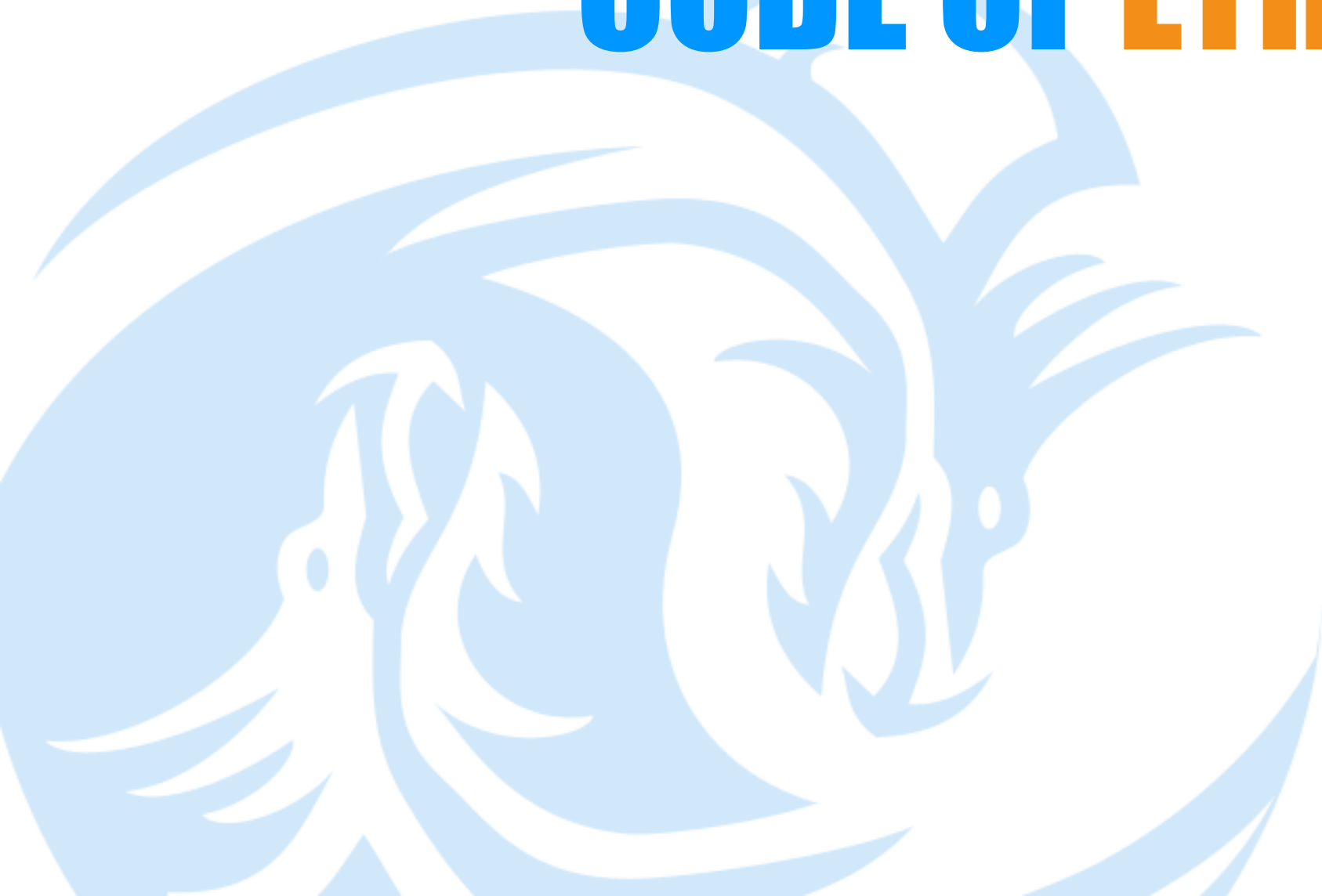


CONFIDENTIAL

CULTURE OF RESPONSIBILITY



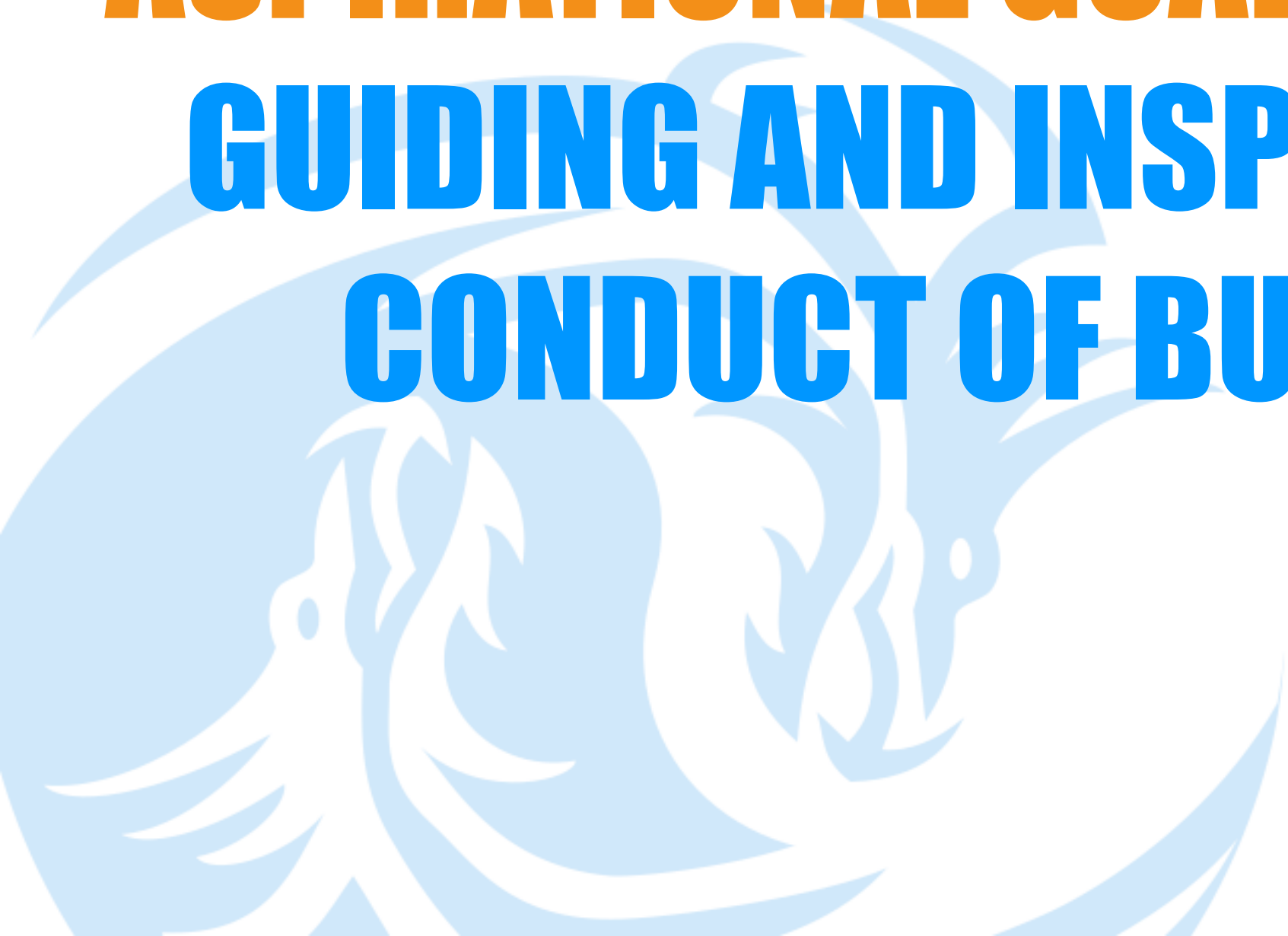
CODE OF ETHICS



A stylized, light blue graphic of a wave or a bird's head in profile, facing right, positioned behind the text.

SIX PRINCIPLES **EIGHT STANDARDS**

**THE PRINCIPLES ARE
ASPIRATIONAL GOALS AIMED AT
GUIDING AND INSPIRING THE
CONDUCT OF BUSINESS**



**THE ETHICAL STANDARDS ARE
ENFORCEABLE RULES FOR THE
DAY-TO-DAY BUSINESS
OPERATIONS.**



PRINCIPLE A:

CLEAN HANDS

Respect all human rights proclaimed by international human rights treaties, including The International Bill of Human Rights, and strive to ensure no complicity in any human rights abuses.

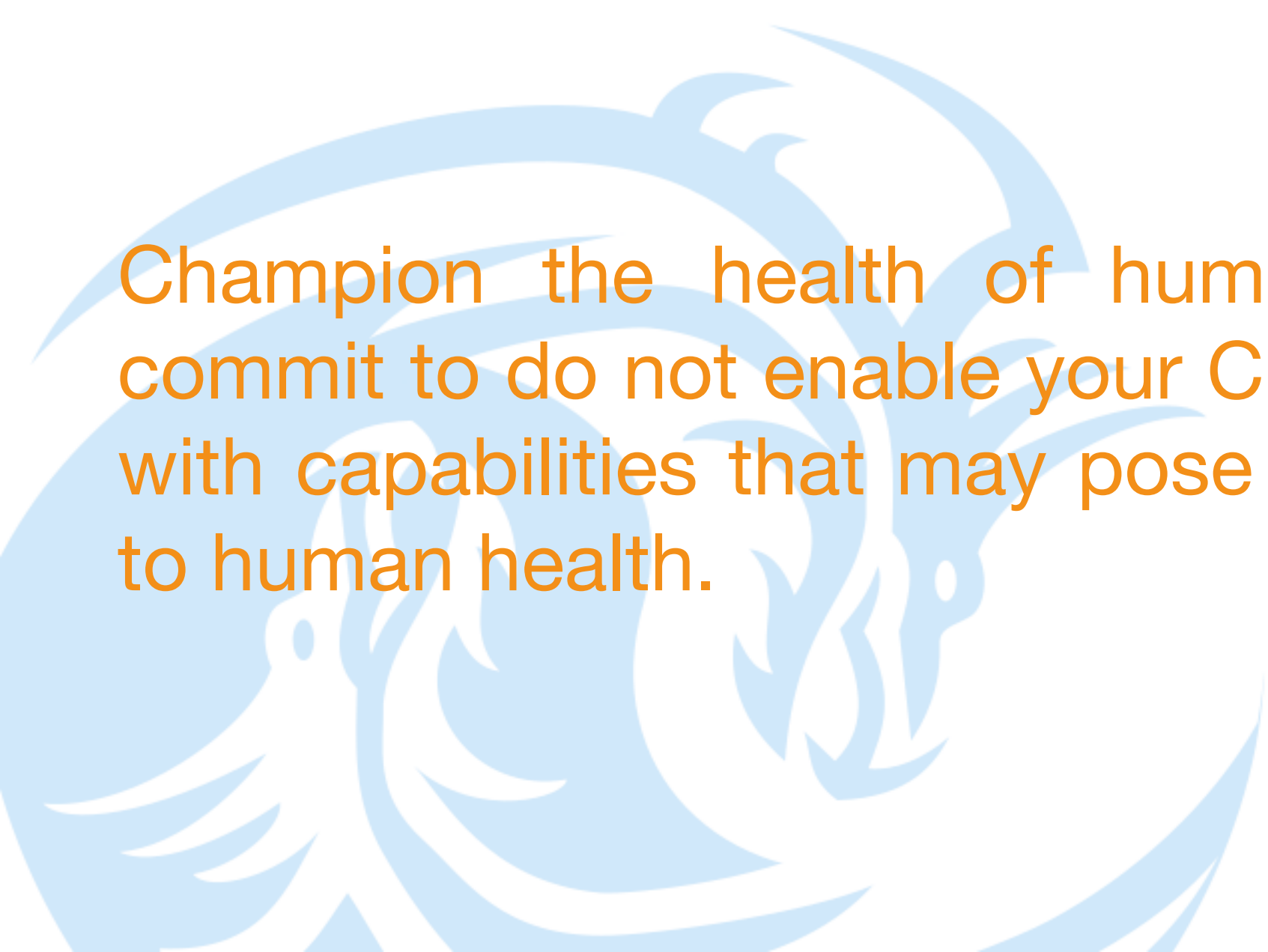
STANDARD 1: VETTING AND MONITORING OF CUSTOMERS

Do not engage in any business with entities known for abusing human rights and reserves the right to suspend or cease business operations with entities found to be involved at a later time in human rights abuses.

PRINCIPLE B:

DO NOT POSE A DANGER TO HUMAN HEALTH

Champion the health of human beings and commit to do not enable your Customer entities with capabilities that may pose a direct danger to human health.



STANDARD 2:

INADMISSIBLE CAPABILITIES

Do not engage in any trade of capabilities that exploit vulnerabilities in medical devices or in systems to which human life is entrusted, unless the Vendor of the affected device or system is the Acquiring Entity or the Acquiring Entity was authorised by the Vendor to be the recipient of the vulnerability disclosure process, vulnerability information, or risk mitigation strategy.

STANDARD 3:

TRADE SECRETS

You will never trade in stolen trade secrets, and require your suppliers to certify that they have independently found the vulnerability and autonomously developed any related technology, and that they are not employees of the targeted software manufacturer, nor have they received access to the confidential information through a disclosure by the same.

OUR GOAL IS TO WRITE
BUG-FREE SOFTWARE.
I'LL PAY A TEN-DOLLAR
BONUS FOR EVERY BUG
YOU FIND AND FIX.



S. ADAMS E-mail: SCOTTADAMS@AOL.COM

YAHOO!
WE'RE
RICH



YES!!!
YES!!!
YES!!!



11/13 © 1995 United Feature Syndicate, Inc. (NYC)

I HOPE
THIS
DRIVES
THE RIGHT
BEHAVIOR.



I'M GONNA
WRITE ME A
NEW MINIVAN
THIS AFTER-
NOON!



PRINCIPLE C:

AVOID CONFLICTS OF INTEREST

Strive to benefit those with whom you do business and take care to avoid possible conflicts of interest that could cause your Company, its Employees, or Contractors to pursue goals not in the interest of the Company business peers.

STANDARD 4:

OVEREXPLOITATION

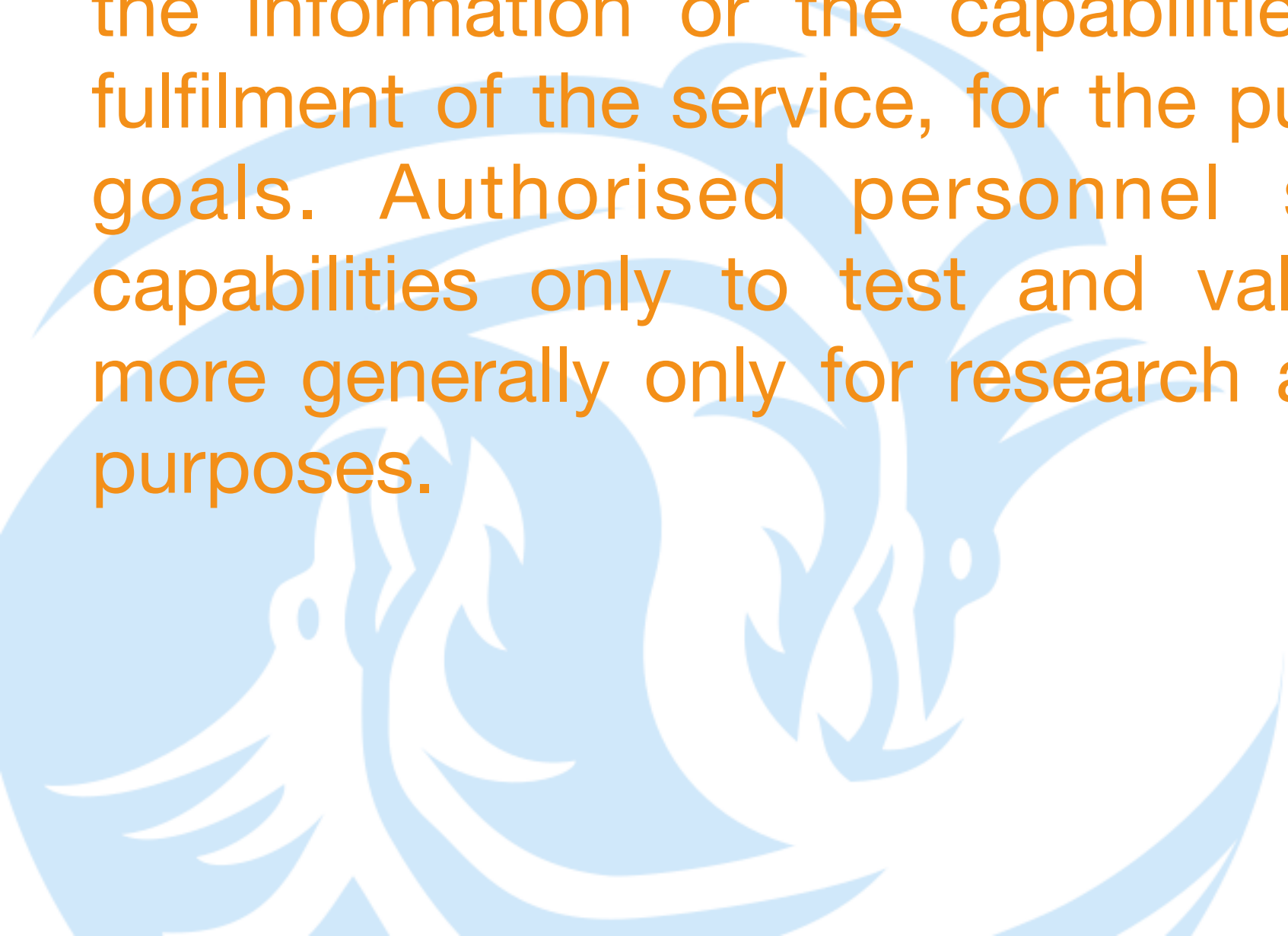
You will protect the value of the traded capabilities. You will specify the maximum number of entities to which the same capabilities may be sold, within a given time-frame (unless in case the capabilities are intended for risk prevention).

Furthermore, you shall strive not to sell a vulnerability to one party, and the technology to defend against that vulnerability to another party which is a likely target of the first.

STANDARD 5:

UNINTENDED USE

Prohibit yourself, employees and contractors to use the information or the capabilities, traded in the fulfilment of the service, for the pursuit of personal goals. Authorised personnel shall use such capabilities only to test and validate them, and more generally only for research and development purposes.



PRINCIPLE D:

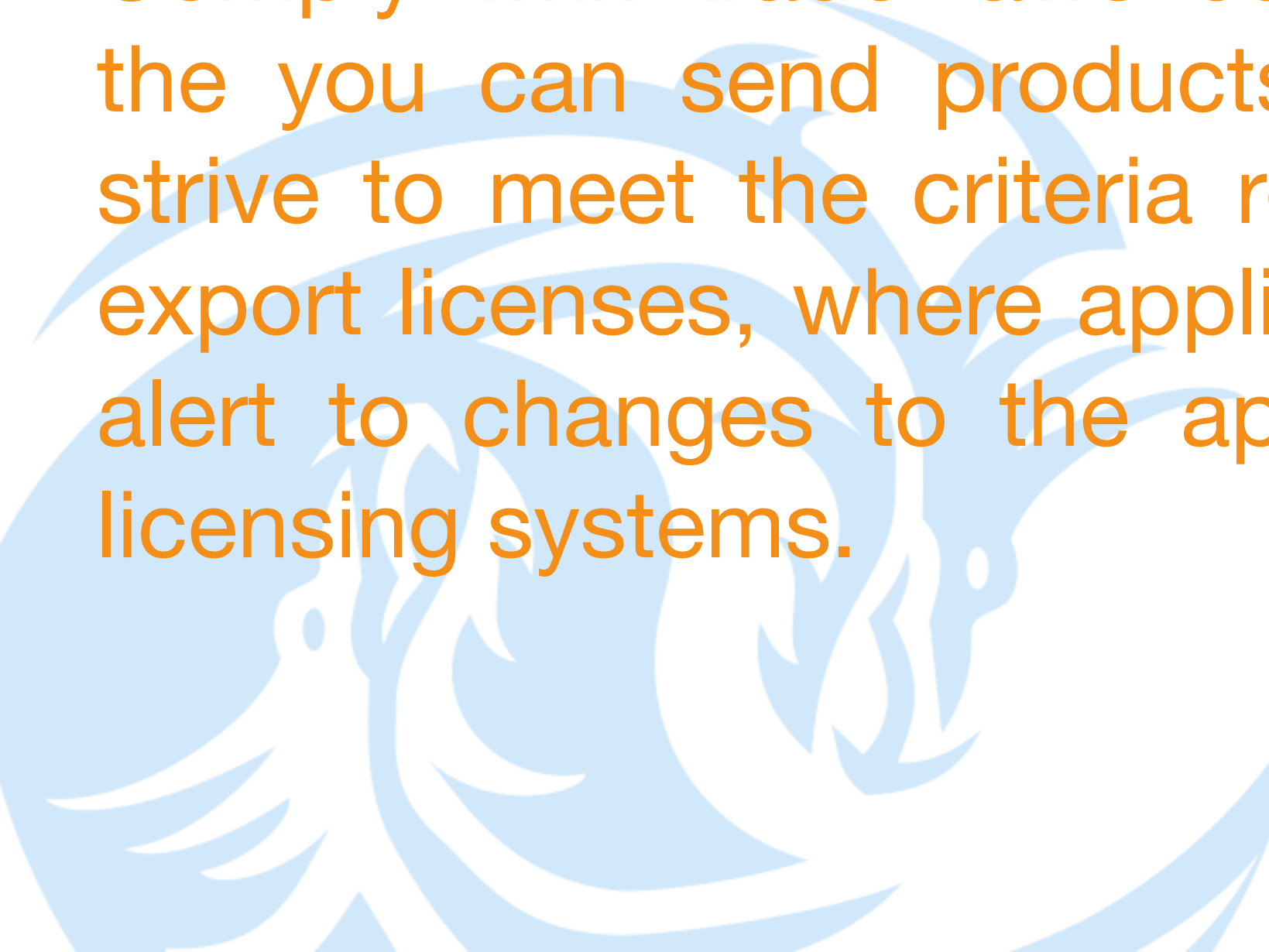
OBEY THE LAW

Comply with all applicable legal requirements and understands the major laws and regulations that apply to your business, including laws related to: trade controls, anti-bribery, competition, trade secret, money laundering and insider trading.

STANDARD 6:

EXPORTING

Comply with trade laws controlling where the you can send products and services, strive to meet the criteria required to hold export licenses, where applicable, and stay alert to changes to the applicable export licensing systems.



PRINCIPLE E:

PRESERVE CONFIDENTIALITY

Protect the confidentiality of the identity of entities you do business with and the confidentiality of the information and intellectual properties received from, or provided to, your business peers in the fulfilment of your Service. At the same time, recognize that the extent and limits of confidentiality may be regulated by applicable laws and regulations.

STANDARD 7:

MAINTAINING CONFIDENTIALITY

At the extent and limits regulated by applicable laws and regulations, preserve the confidentiality of the identity of entities you do business with. Restrict access to the information and the intellectual property received from or provided to your business partners on a need-to-know basis, enforcing a principle of least privilege

PRINCIPLE F: DOCTRINE OF DOUBLE EFFECT AND DUAL USE

Acknowledge that the capabilities you provide may be used within goods that, just like any and all information security tools, are inherently dual purpose and potentially dual use, and therefore may serve also military purposes, police investigations and the like; the military use of the traded capabilities may have a double effect: the intended effect and the foreseen but genuinely unintended consequence. While discouraging against harmful side effects, you acknowledge the inherent duality of the effects resulting from the use of those capabilities and you trade them, unless they are in conflict with other principles set forth in the present Ethics Code.

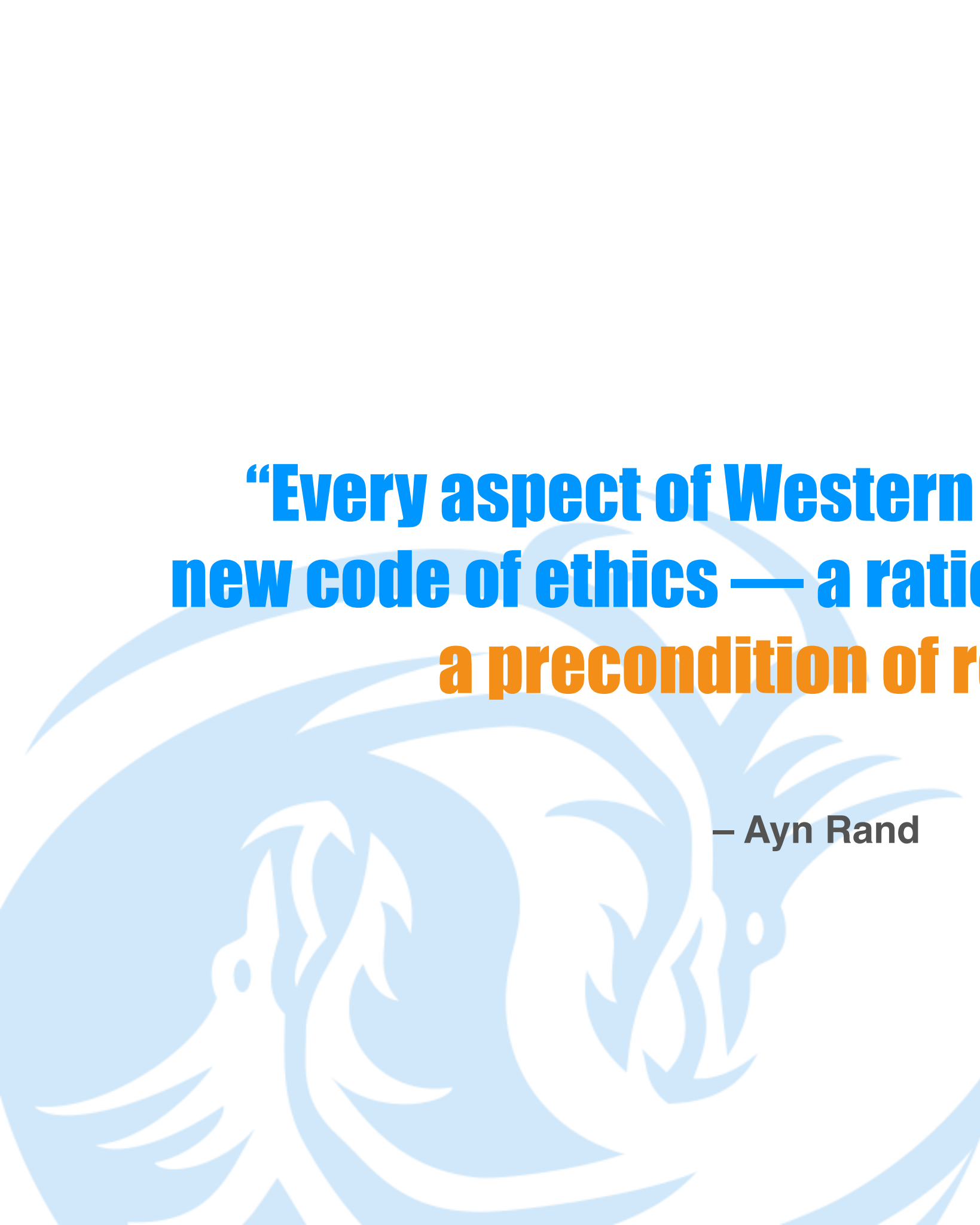
STANDARD 8: DUALITY

Acknowledge that the capabilities you provide can be used within goods that are inherently dual purpose and accept to supply them, as long as it is foreseeable that those capabilities will be used only for legitimate purposes in line with international standards for the respect of human rights, and unless their trade is in conflict with principles set out in the present Ethics Code.

CONCLUDING REMARKS **AND DEBATE**





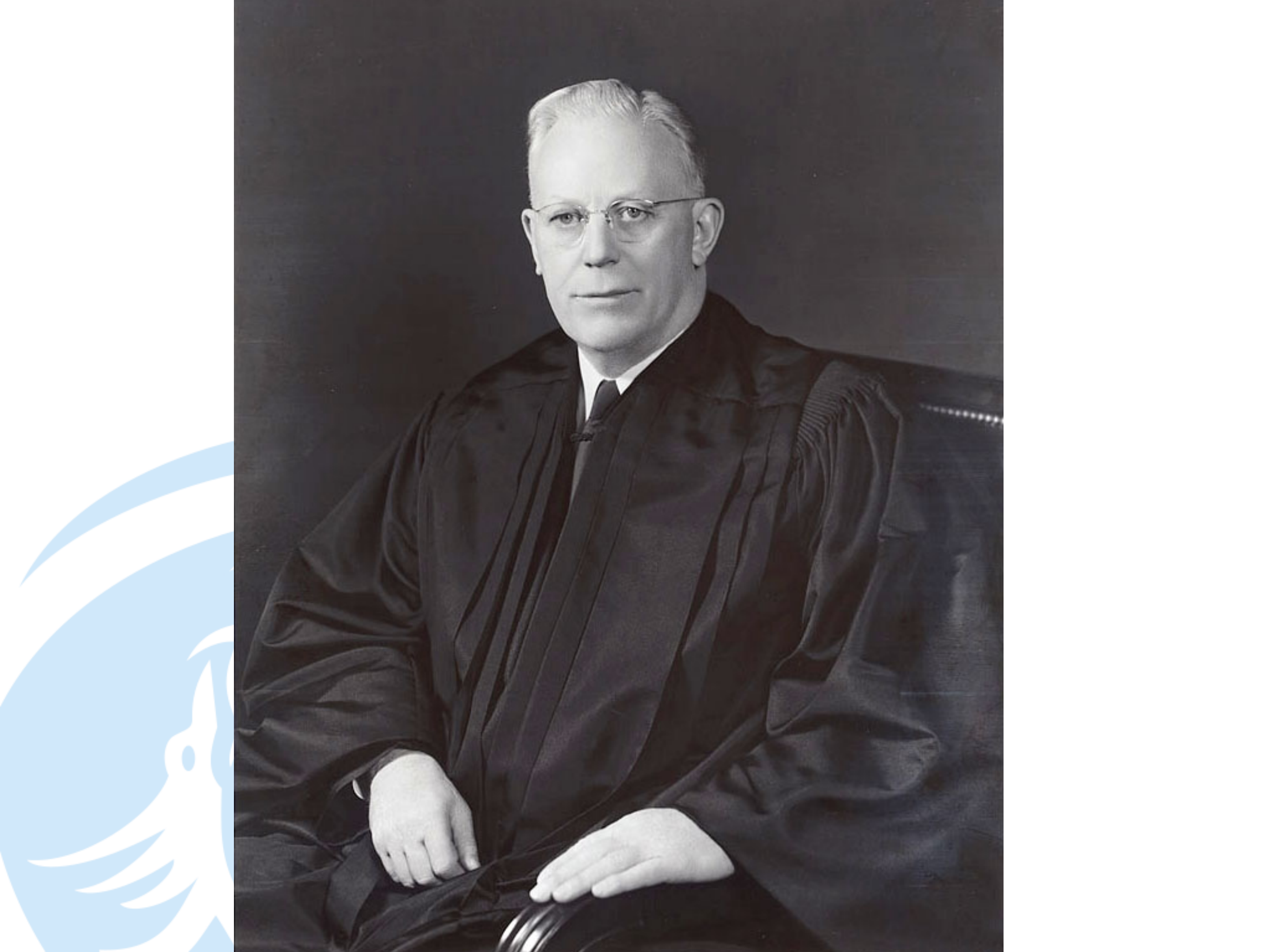


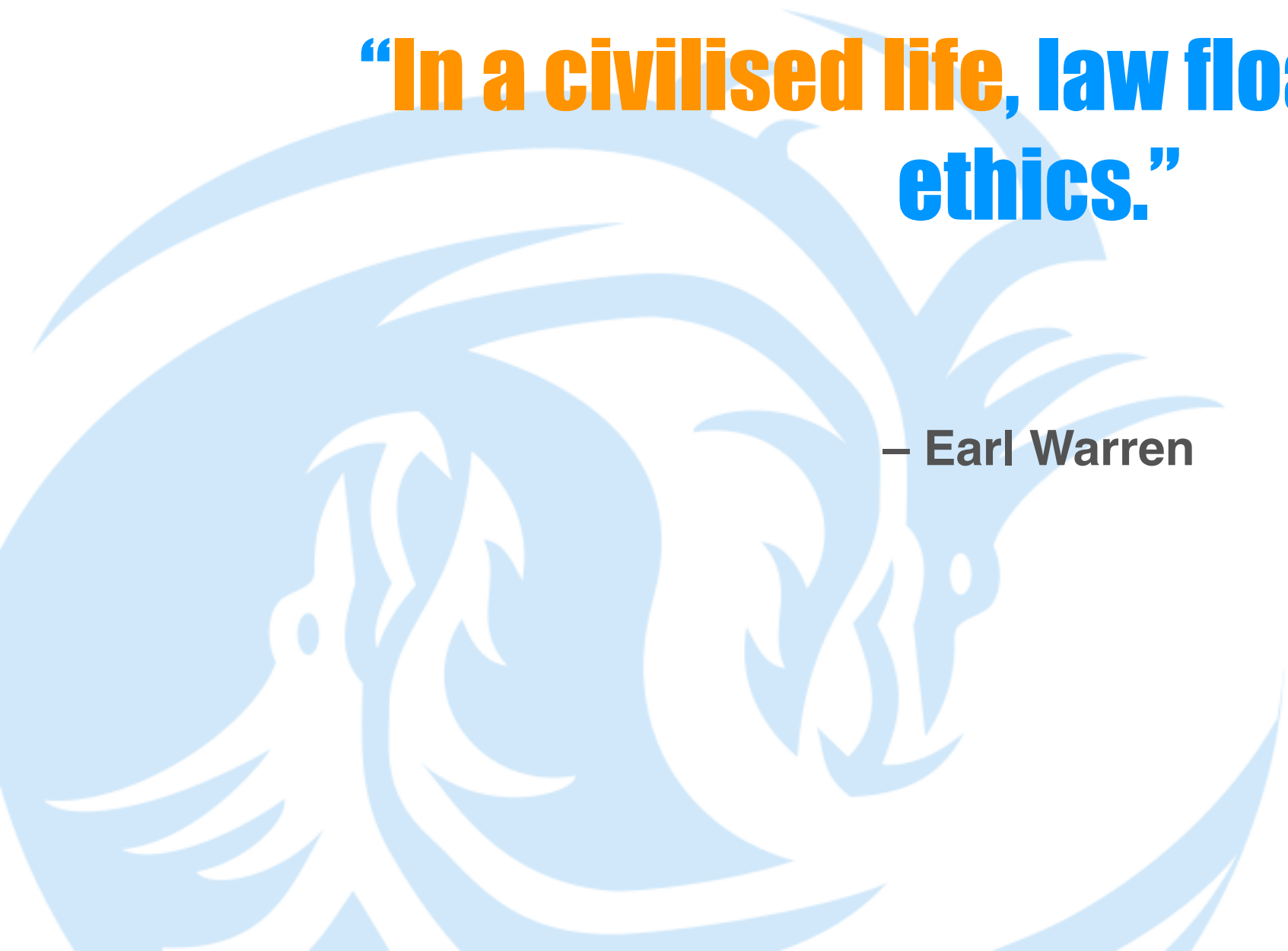
“Every aspect of Western culture needs a new code of ethics — a rational ethics — as a precondition of rebirth.”

— Ayn Rand

**Every aspect of the vulnerabilities
supply chain needs a new code of ethics
— a rational ethics — as a precondition
of rebirth.**







“In a civilised life, law floats in a sea of ethics.”

– Earl Warren



“Expanding the scope of ethical deliberation over new technology may seem like a daunting prospect bound to impede innovation.”

– Steven Aftergood

THANK YOU!



ANY QUESTIONS?





Zeronomicom

Disclosing Unknowns