



REGULATORY OPTIONS FOR THE GLOBAL TRADE IN ZERO-DAY VULNERABILITIES

MAILYN FIDLER
STANFORD UNIVERSITY
SECOND ANNUAL CONFERENCE ON GOVERNANCE OF EMERGING TECHNOLOGIES
5.28.14

When you sell:

- A zero-day vulnerability, you sell **knowledge** of existing flaw
- A zero-day exploit, you sell **new code** that takes advantage of an existing vulnerability



White Market

Google

\$100-100,000

Average around \$2000

mozilla



Black Market

\$4,000-75,000

Wide variability, little data

Gray Market

\$16,000-250,000

Average around \$20,000-50,000



Global Gray Market for Zero-Day Vulns



Confirmed Government Buyers

- U.S.A
- U.K.
- Israel
- Brazil
- India
- Malaysia
- Singapore
- Russia
- North Korea
- Iran

Case Studies

DOMESTIC

Criminalization

Export Controls

Oversight

INTERNATIONAL

International Law

Voluntary collective action

Collective defense action

Case Studies

DOMESTIC

Criminalization

Export Controls

OVERSIGHT

INTERNATIONAL

International Law

VOLUNTARY COLLECTIVE ACTION

Collective defense action

OVERSIGHT

Administration Vulnerability Disclosure Policy

- “***Biased** toward responsibly disclosing such vulnerabilities*” (NYT)
- “*Broad **exception** for ‘a clear national security or law enforcement need’*” (NYT)
- “*Re-invigorated our efforts to implement **existing** policy with respect to disclosing vulnerabilities.*” (WH Blog)

OVERSIGHT HOLES:
OVERSIGHT OF PURCHASED VULNS
POST-USE REVIEW PROCESS

VOLUNTARY COLLECTIVE ACTION: THE WASSENAAR ARRANGEMENT

INTRUSION SOFTWARE?





mfidler@stanford.edu

<http://purl.stanford.edu/zs241cm7504>