# Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity $(IC)^3$


## 3 Sept 2014

# Advancing Cybersecurity Using System Dynamics Simulation Modeling For Analyzing & Disrupting Cybercrime Ecosystem & Vulnerability Markets

Massachusetts Institute of Technology

James Houghton
Michael Siegel

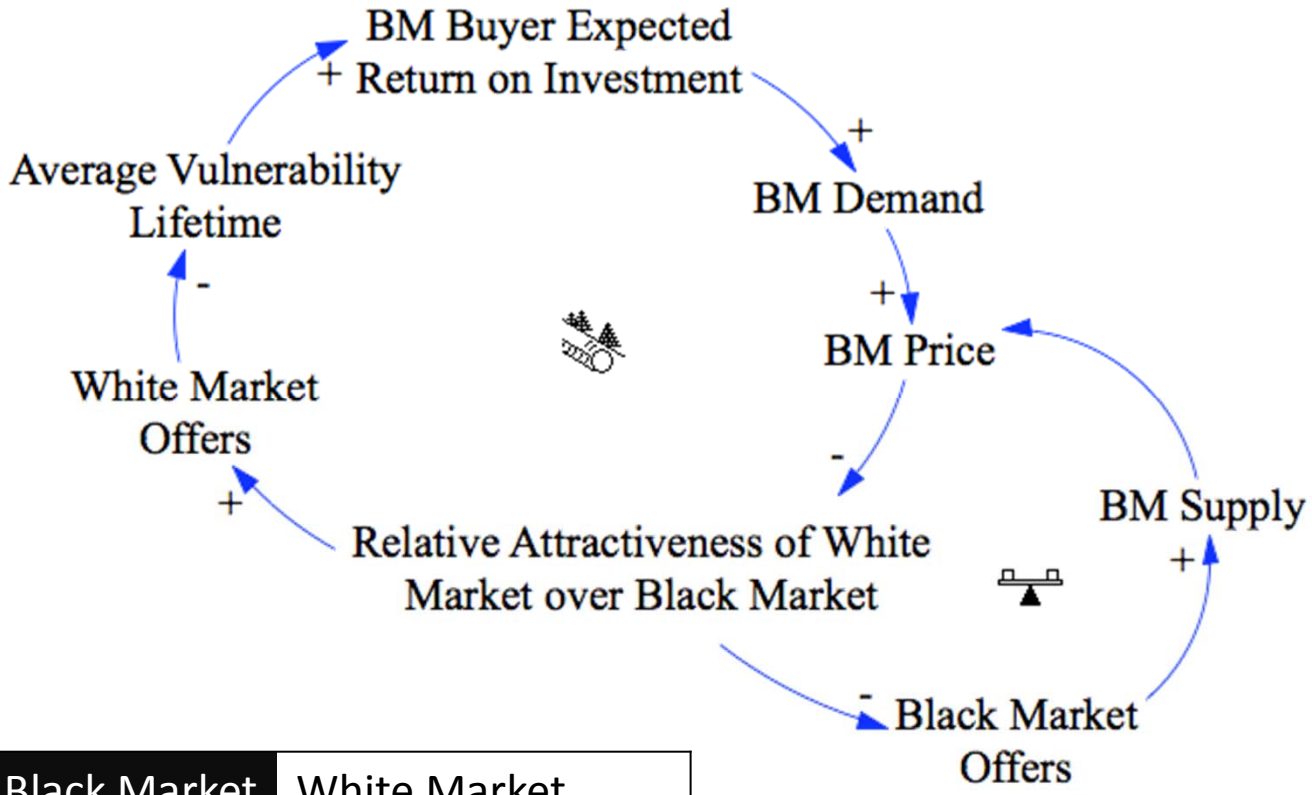
MITSloan MANAGEMENT

# Resolving Emergent Issues In Cyber Security: Vulnerability Markets

# How do white markets influence black market pricing?

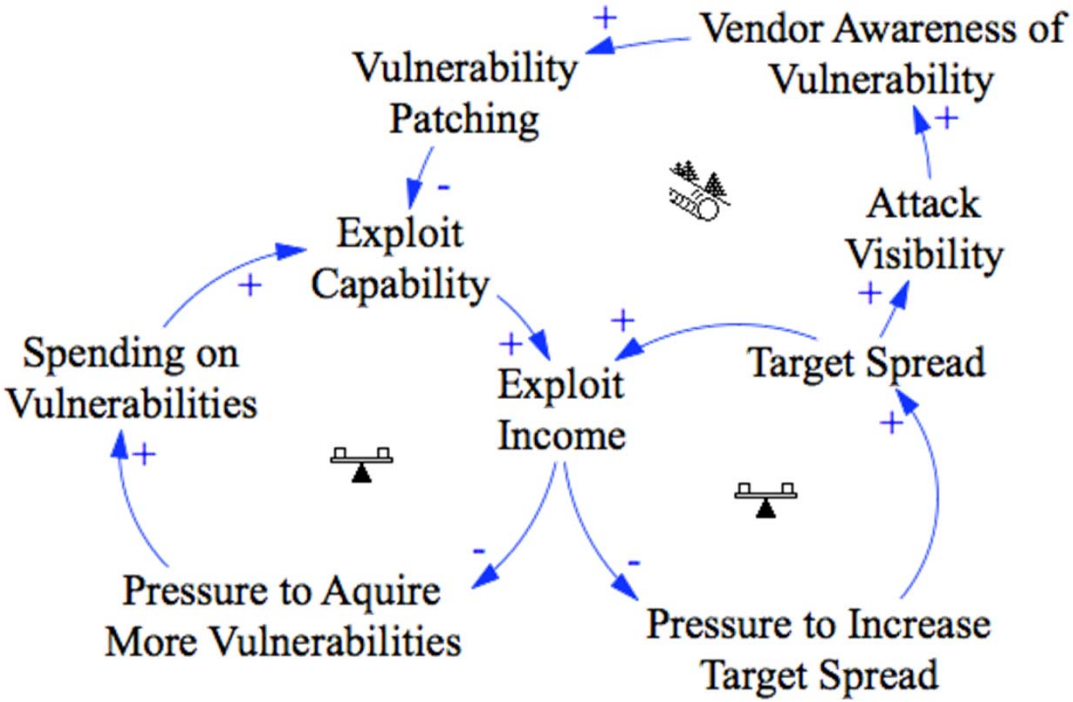
An exploit's price factors in both how widely the target software is used as well as the difficulty of cracking it.

Greenberg - Forbes




| | Black Market (Forbes 2012) | White Market (2014) |
|---|---|---|
| IOS | $100k-$250k | $0k |
| Android | $30k-$60k | $0.5k – $3.1k |
| MS Windows | $60k-$120k | $50-$100k |
| Internet Explorer | $80k-$200k | 11k |

# What is the lifecycle of cybercrime?




'Selling a bug to the Russian mafia guarantees it will be dead in no time, and they pay very little money … They monetize exploits in the most brutal and mediocre way possible…'

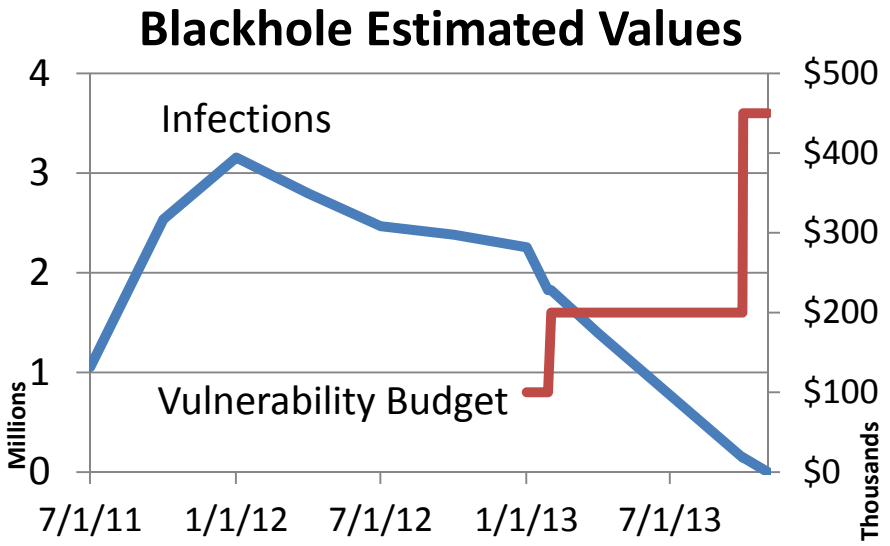
-Grugq, third party broker

Greenberg, Forbes

'We are setting aside a $100K budget to purchase browser and browser plug-in vulnerabilities, which are going to be used exclusively by us, without being released to public'

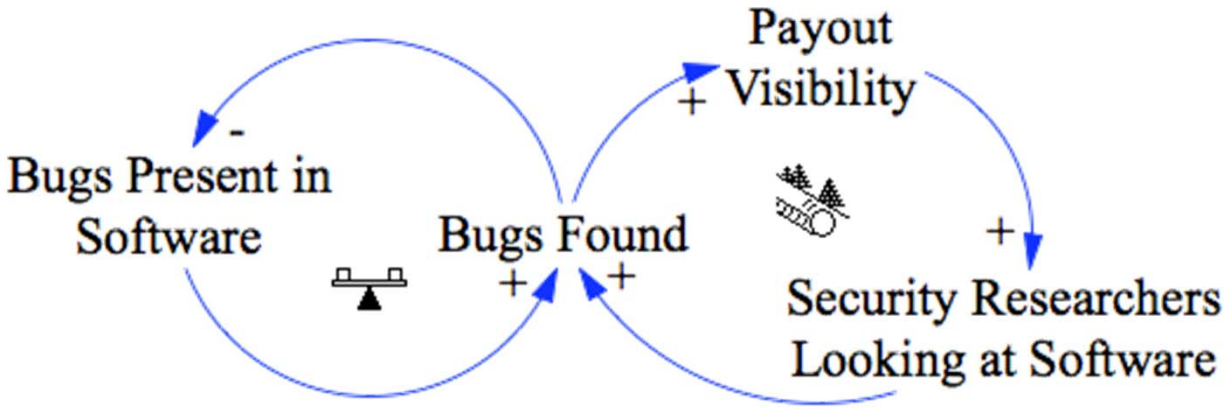
- Paunch, Author of Blackhole, Jan '13

Krebs on Security




Data from Microsoft Security Bulletins, Krebs on

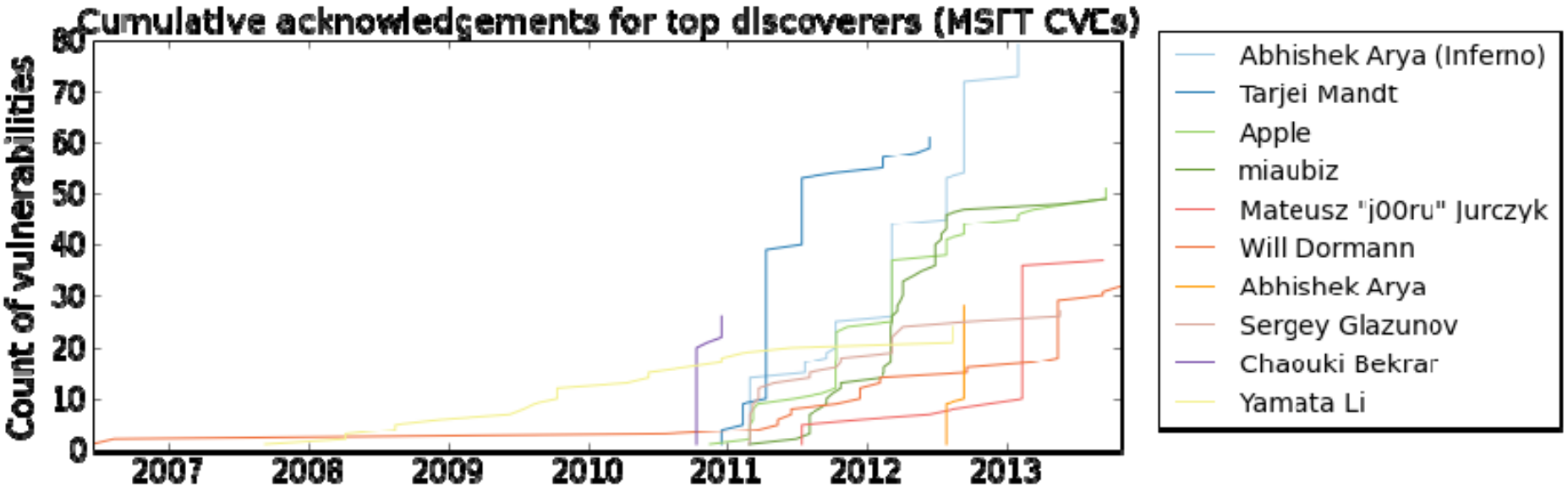
# How do bug bounty programs influence vulnerability supply?

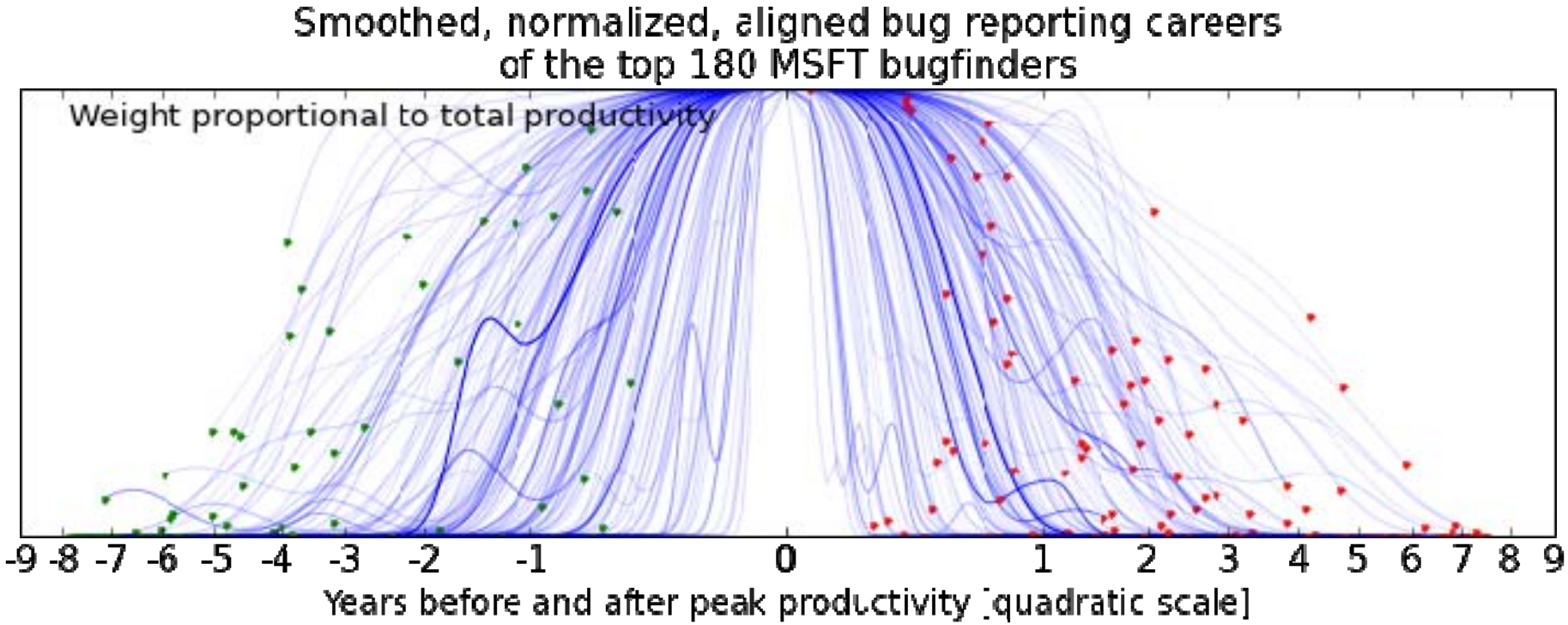



**Bounty Evolution: $100,000 for New Mitigation Bypass Techniques Wanted Dead or Alive**

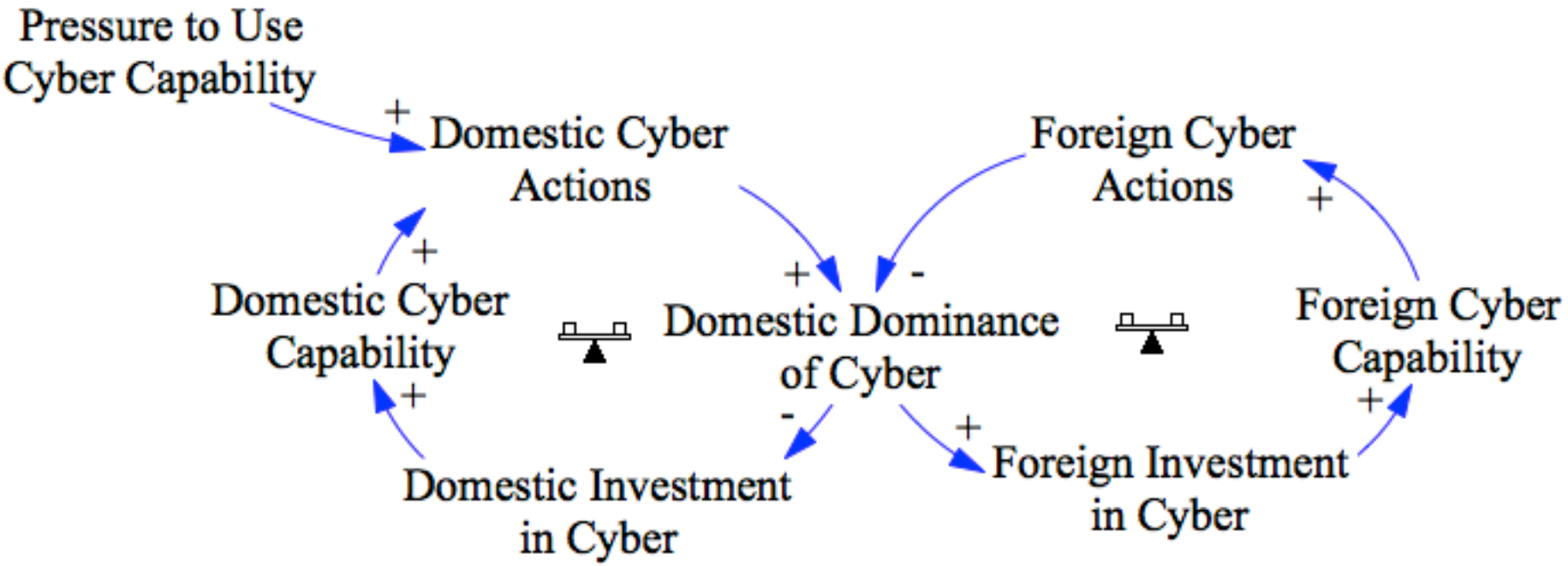
"Microsoft is announcing the first evolution of its bounty programs, first announced in June of 2013. We are expanding the pool of talent who can participate and submit novel mitigation bypass techniques and defensive ideas to include responders and forensic experts who find active attacks in the wild."

- Katie Moussouris, BlueHat Blog


Cumulative acknowledgements for top discoverers (MSFT CVEs)
Count of vulnerabilities
0
10
20
30
40
50
60
70
80
2007
2008
2009
2010
2011
2012
2013
Abhishek Arya (Inferno)
Tarjei Mandt
Apple
miaubiz
Mateusz "j00ru" Jurczyk
Will Dormann
Abhishek Arya
Sergey Glazunov
Chaouki Bekrar
Yamata Li


Smoothed, normalized, aligned bug reporting careers
of the top 180 MSFT bugfinders
Weight proportional to total productivity
-9 -8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9
Years before and after peak productivity [quadratic scale]

# How does State investment in cyber capability influence foreign behavior?

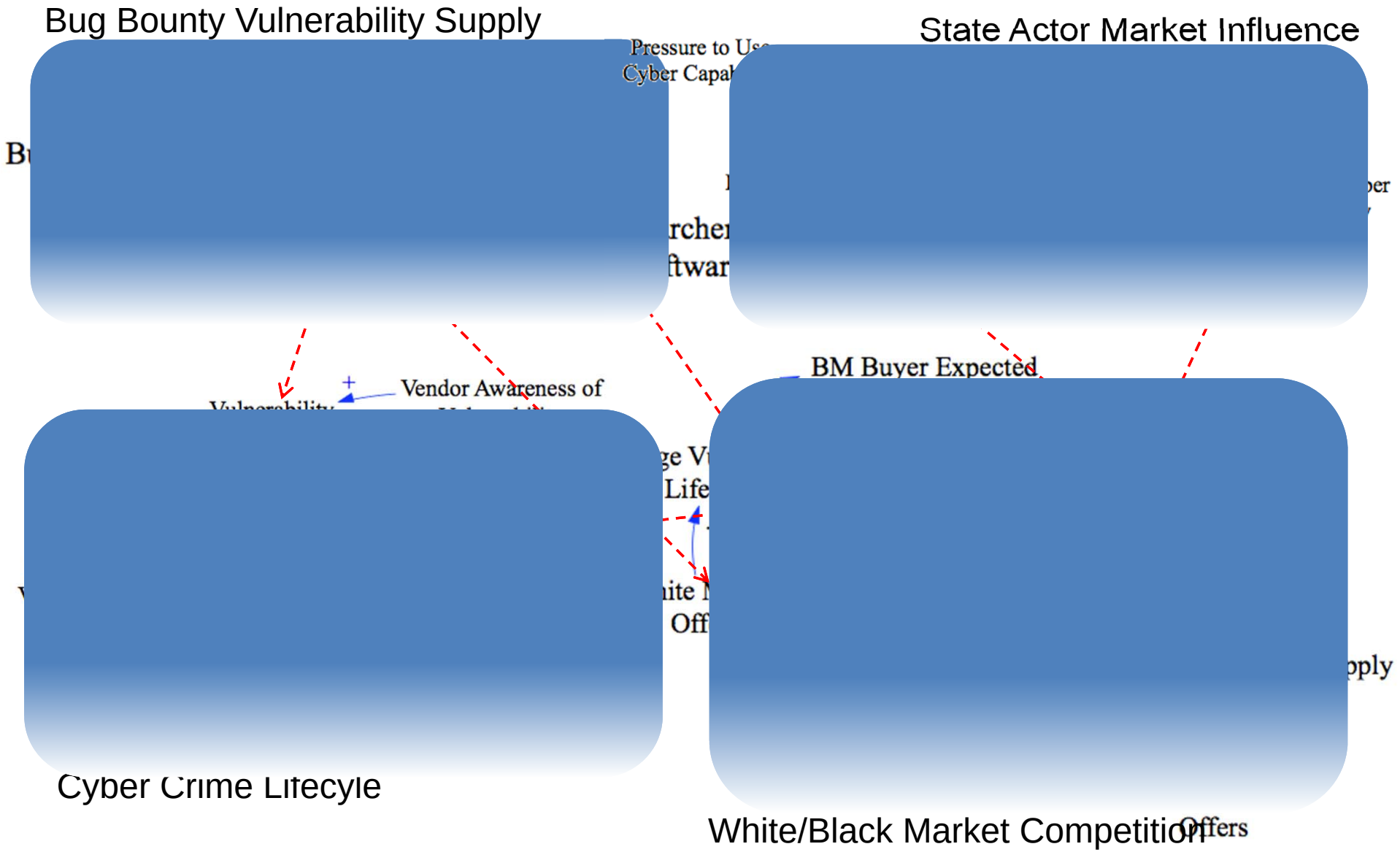



"The Chinese are conducting espionage on a massive scale. [If we] ban sales of … exploits to the U.S. and European allies … the only possible outcome is that the Chinese will increase their internal production and skills and the…West will fall behind."

-Grugq, third party broker

Greenberg, Forbes

# Cyber Security Challenge: Resolving Problems As Part Of A Larger System



# Summary

- Cybersecurity solutions require a holistic approach
- Systems modeling considers, behavior, management, policy and technology
- The case of patching and software quality provide insights into timing and approaches
- Bug bounty programs and vulnerability markets have significant effect on security and the cyber ecosystem