Operacje ofensywne w cyberprzestrzeni
Mity a rzeczywistość

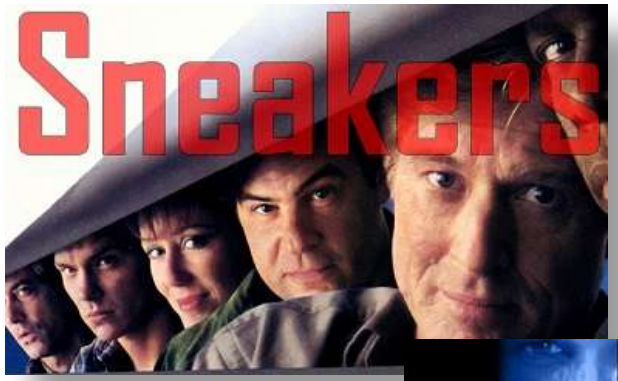
Błażej Kantak, x33fcon

III Konferencja Naukowa
Bezpieczeństwo Informacyjne w Obszarze Cyberprzestrzeni
Akademia Marynarki Wojennej w Gdyni

Mitologia

Mitologia...


blackhat
"I can target Anyone, Anything... Anywhere"

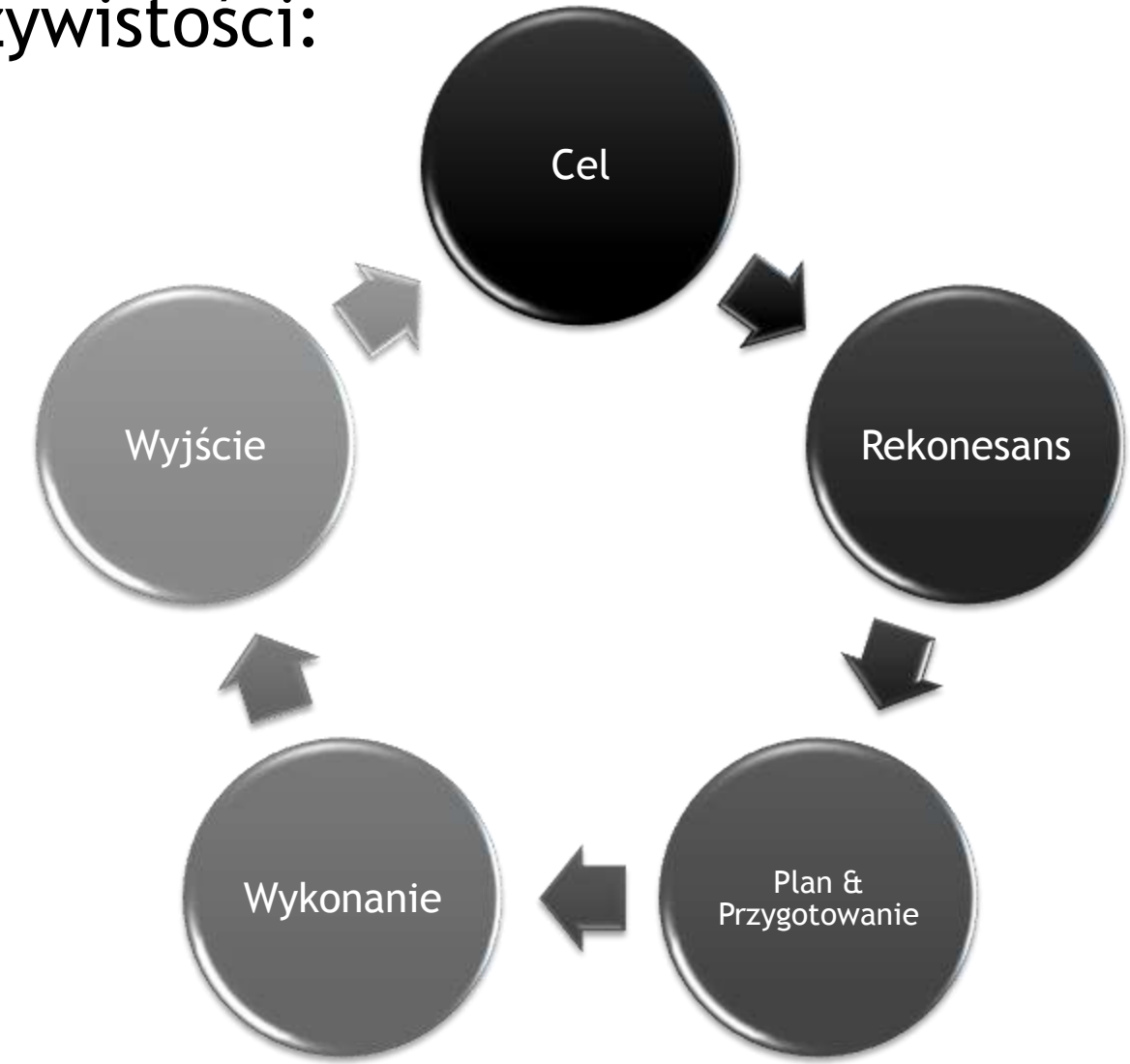

Sneakers


HACKERS

Mit #1.
Potrzeba ułamka sekundy aby przejąć sieć

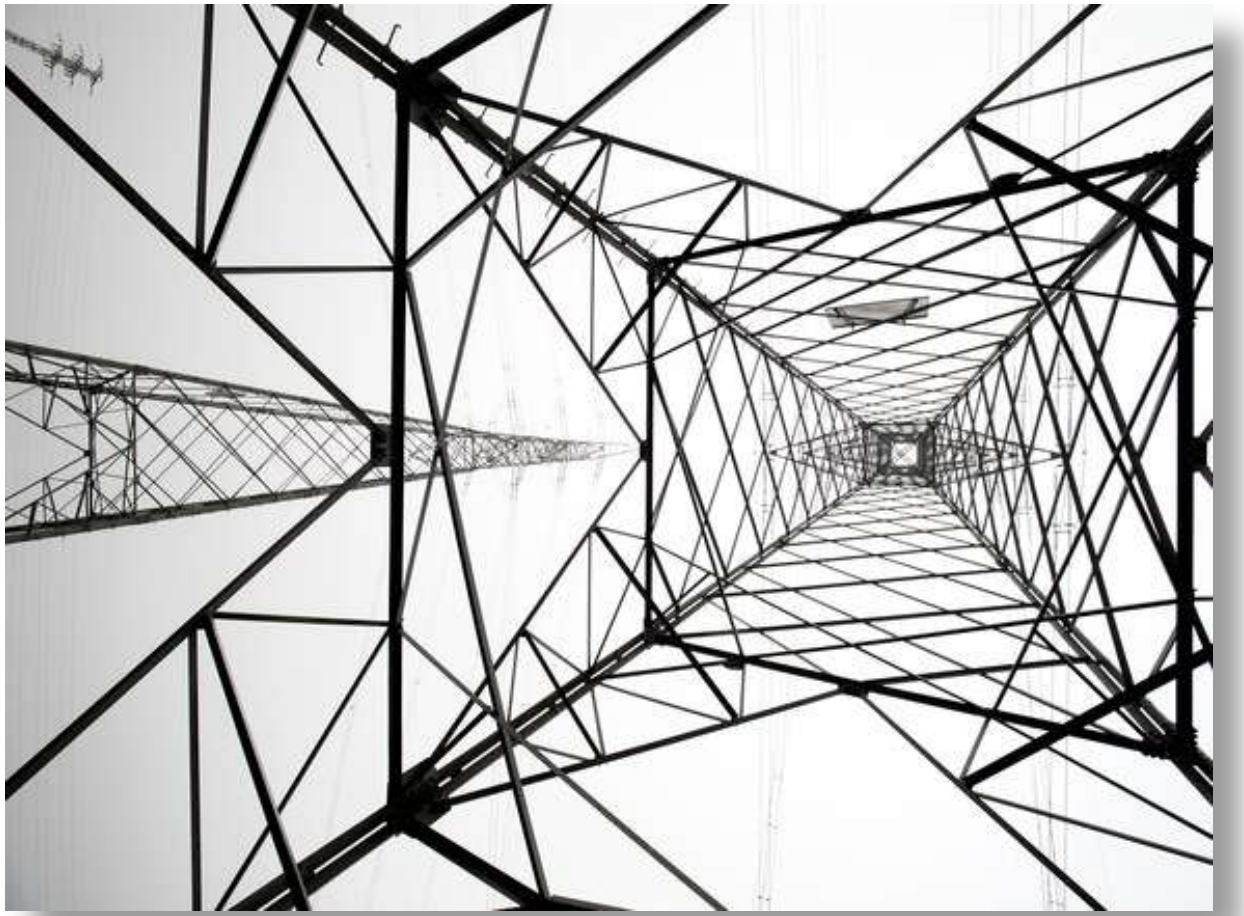
Mit #1. Pif-paf, bang?

W rzeczywistości:



Mit #1. Pif-paf, bang?

Przykład: Ukraina 2015/12/23



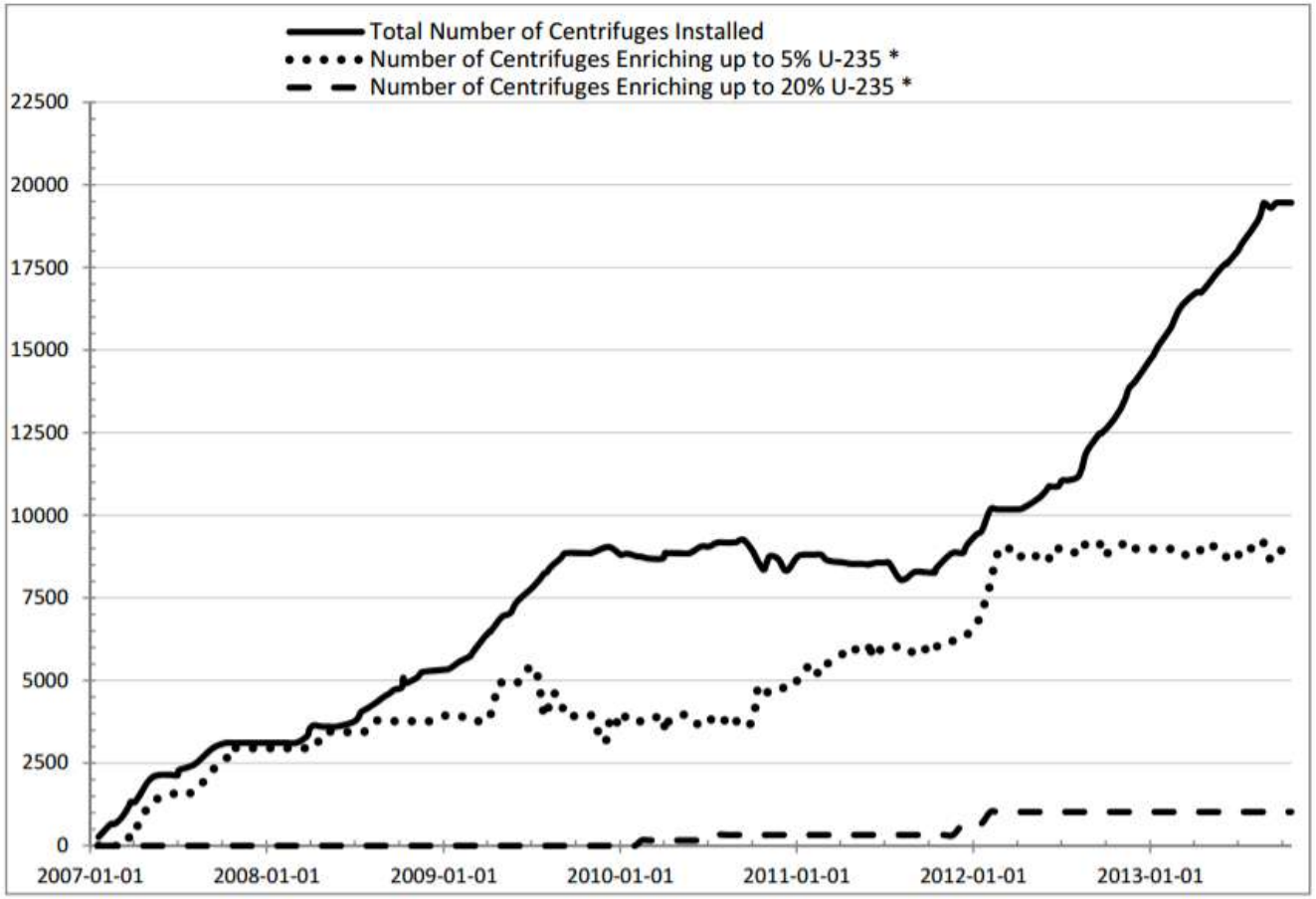
Czas przywrócenia usługi: <24h, efekt psychologiczny

Mit #1. Pif-paf, bang?

Przykład: Olimpic Games/Stuxnet

Efekty (2007-2013)

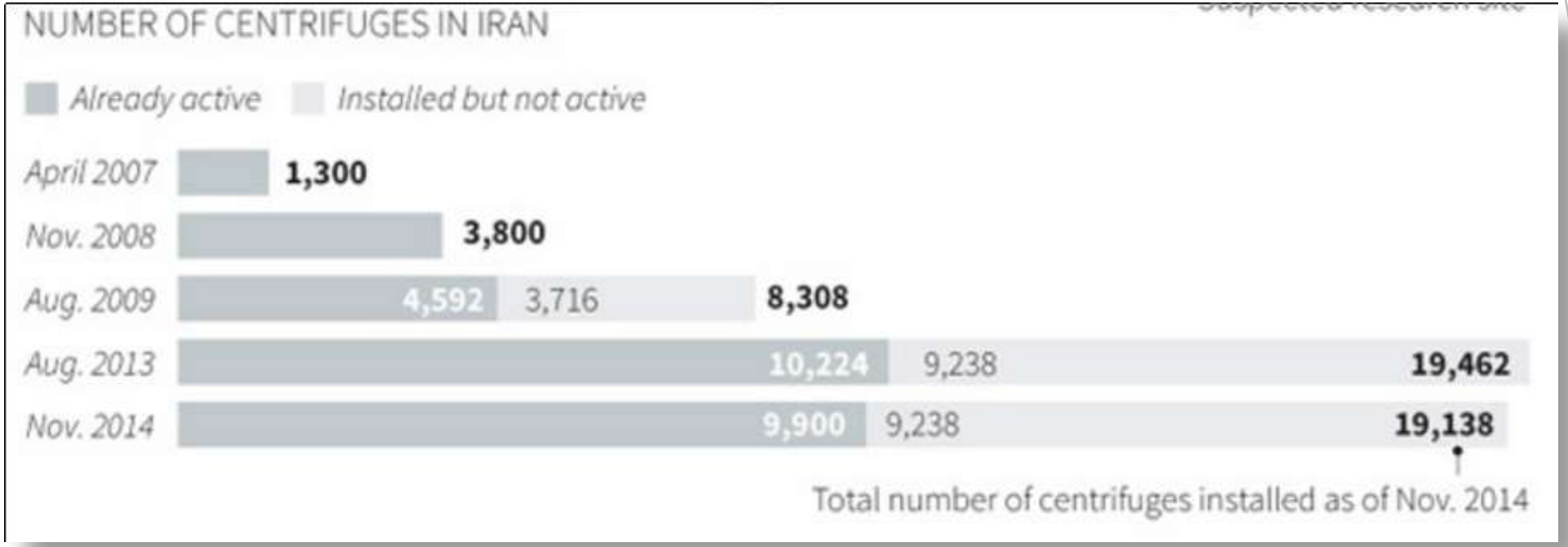
Figure 1: Status of Centrifuges in Iran



Note 1: Centrifuges involved in R&D activities are not included.
**Not all of the centrifuges fed with UF_6 may have been working.*

https://www.iaea.org/sites/default/files/gov2013-56.pdf

Efekty (2013-2014)



http://blogs.reuters.com/data-dive/2015/03/19/processing-irans-centrifuge-numbers/

Mit #2.
Adwersarze są „mądrzejsi”

Mit #2. Uberhackers?

W rzeczywistości:

- to też są ludzie
- typowe błędy w narzędziach (memory corruption)
- błędy w czasie misji (OpSec)
- znajomość ataku bez potrzebnej wiedzy o technologii

Prawdziła „siła” pochodzi od tego, jak dobrze grupa jest zorganizowana i od ludzi, którzy tworzą narzędzia.

Mit #3.

Adwersarze zawsze wykorzystują błędy 0-day

Mit #3. 0-days?

W rzeczywistości:

- wyjątkowe sytuacje
- błędy w oprogramowaniu vs błędy człowieka
- wykorzystanie narzędzi domyślnych/zaufanych
- typowe błędy: hasła, hasła, hasła...
- znane błędy, złe konfiguracje

Mit #4?

Dla adwersarza wystarczy jedna podatność, obrońca musi znaleźć wszystkie

Mit #4. Asymetria czasu?

W rzeczywistości:

- prawda tylko do momentu włamania
- sytuacja ulega odwróceniu

Obrońcy wystaczy jeden błąd adwersarza, aby go wykryć

Mit #5?

„Chmura” jest/nie jest* bezpieczna

* niepotrzebne skreślić

~~Mit~~ #5. Chmura/nie-Chmura?

Kwestia zaufania?

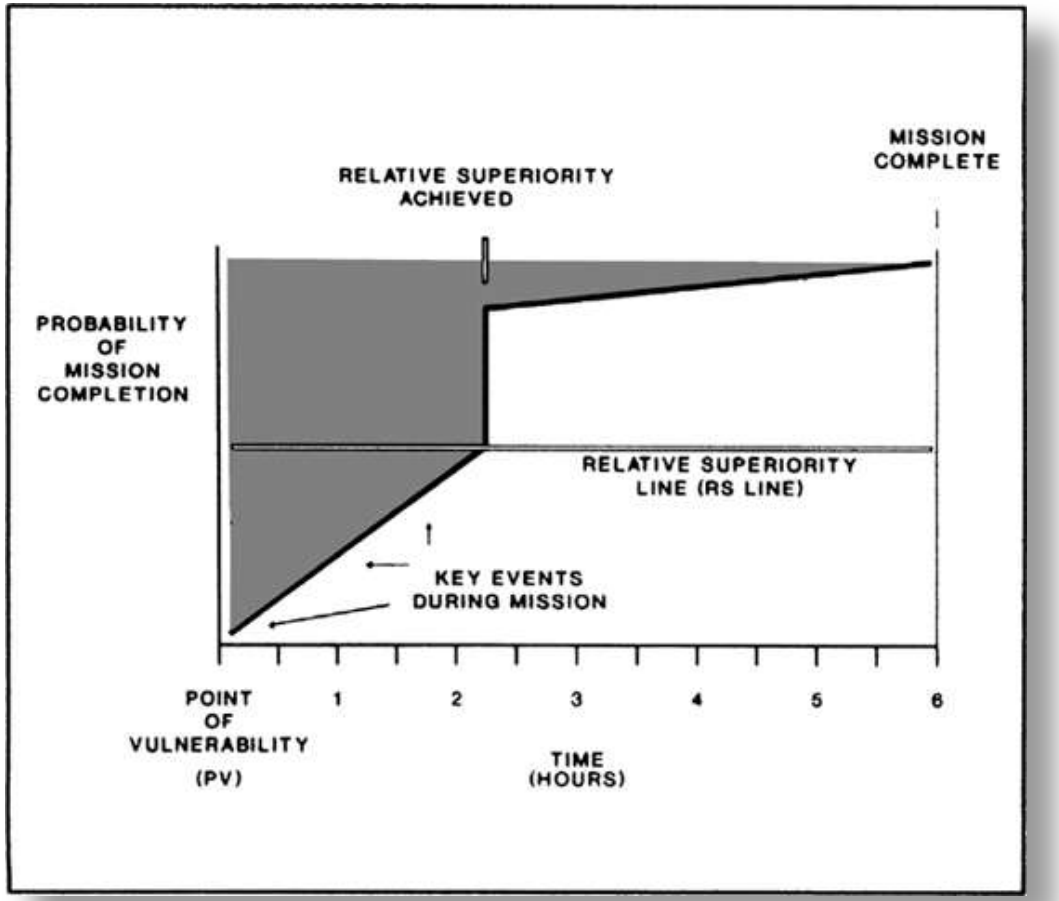
- Zapewnienia dostawcy? Gwarancja?
- Certyfikacja? (np. PCI DSS)
- Audyt?
- Testy penetracyjne?
- Czy nadal kontrolujemy dane?
- Czy infrastruktura dostawcy może zostać wykorzystana przeciwko nam np. w phishingu?
- Jak zapewnić wykrywanie włamań? Jak reagować?
- Jak zrobić digital forensics?
- Czy infrastruktura musi być dostępna „wszędzie”?

Dla adwersarza nie ma (w zasadzie) znaczenia, gdzie są dane

Operacje w cyberprzestrzeni
vs
Operacje specjalne

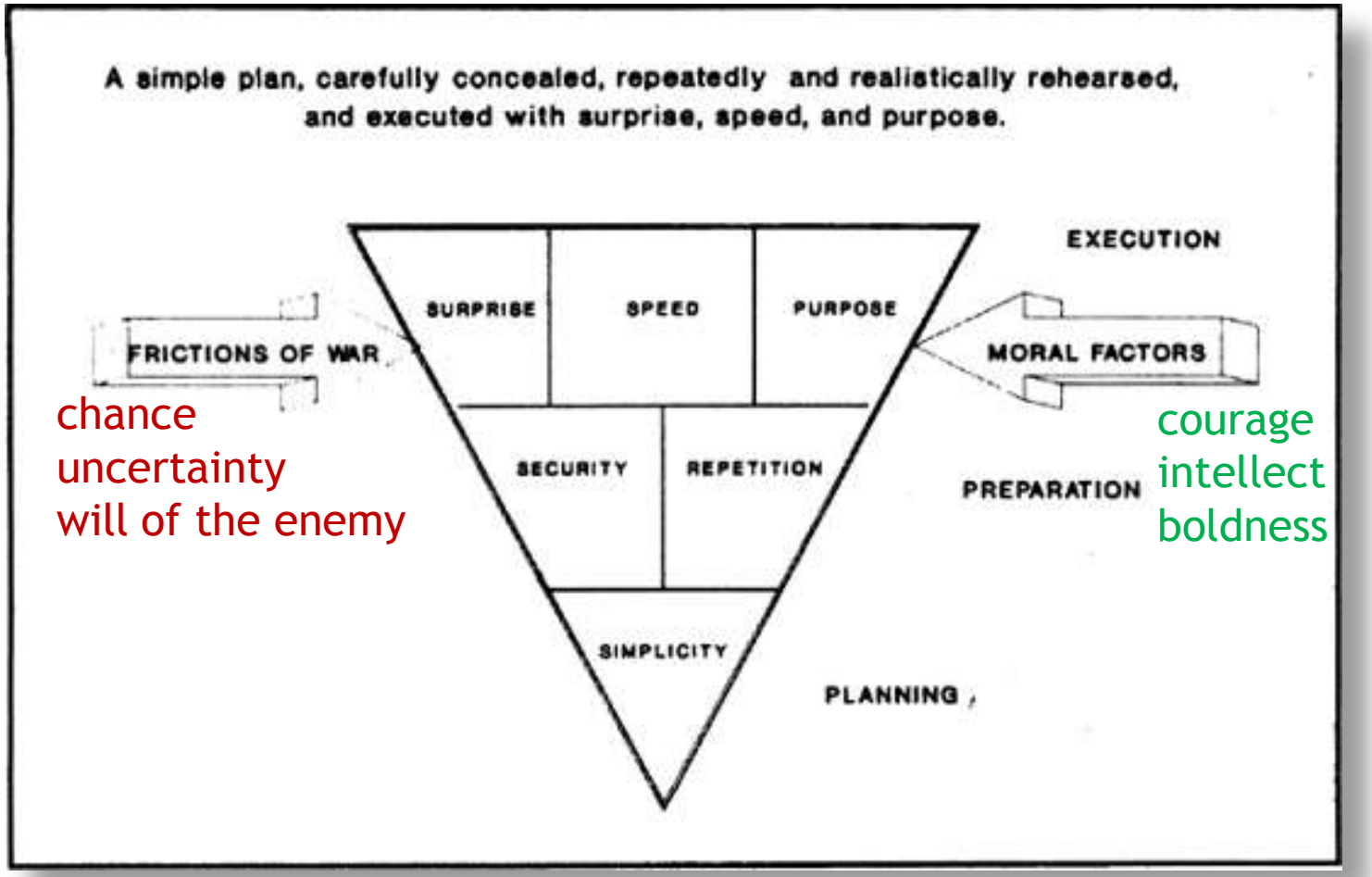
CyberOps vs SpecOps

W wielu aspektach przypominają operacje specjalne



William H. McRaven (1996). Spec Ops: Case Studies in Special Operations Warfare. Theory and Practice.

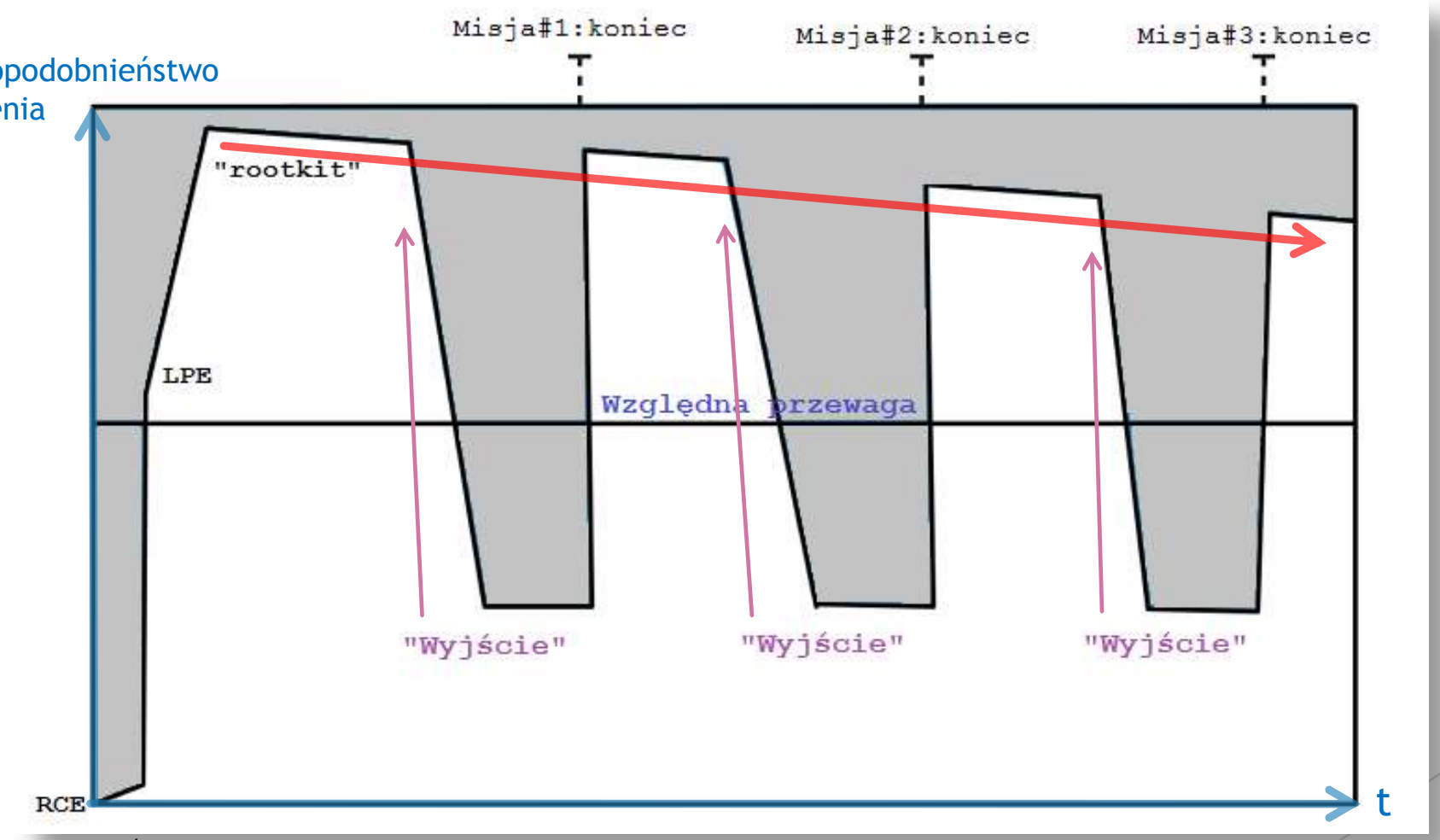
CyberOps vs SpecOps



William H. McRaven (1996). Spec Ops: Case Studies in Special Operations Warfare. Theory and Practice.

CyberOps vs SpecOps

Typowa operacja ofensywna:



Źródło: www.recordedfuture.com

Dziękuję za uwagę

@x33fcon
https://www.x33fcon.com