# SİBER OLAYLARDA MEŞRU MÜDAFAA

OĞUZ KAAN PEHLİVAN

24.04.2014

HACETTEPE ÜNİVERSİTESİ,
SİBER GÜVENLİK VE ULUSLARARASI POLİTİKA KONFERANSI

# SUNUM PLANI

- Sorular
- Meşru Müdafaa Doktrİni
- Self-Help Doktrİni
- Sonuç

# SORULAR

- Saldırının çeşidi? Siber casusluk, siber suç, siber terörizm ya haktivism?
- Verilen zararın boyutları?
- Saldırının arkasında kim var? Hackerlar-Cracker, Suç örgütü, devlet?

- BM Şarti madde 51 : «Bu antlaşmanin hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahli bir saldiriya hedef olmasi halinde, Güvenlik Konseyi uluslararasi barış ve güvenliğin korunmasi için gerekli önlemleri alincaya kadar, bu üyenin doğal olan bireysel ya da müşterek meşru müdafaa hakkina halel getirmez»

  - Sinir Aşan Boyut
  - Silahli Saldiri

# 1- Silahli Saldiri olmali

- Kinetik olmasi gerekir mi?
- UAD, Nükleer Silahlar Karari, «saldiri araçlarinin o saldiriyi silahli olarak nitelemek için önemli olmadiğini»
- Devlet Uygulamasi: «Kimyasal ve biyolojik saldirilar, felaket sonuçlar yaratabileceği için meşru müdafaa hakkinin konusu olur»
- Siber saldirilar da bu potansiyelde

- Boyut ve Etki Testi (Scale and effect Test)
  - Bir eylemin silahli saldiri boyutuna ulaşip ulaşmadiği
  - 2 Yaklaşim: Saldirinin Doğasi (Öldürücü ve Yikici) & Saldirinin Sonuçlari ve Etkisi
  - Siber saldirilarda: yaralama, ölüm, maddi zarar ortaya çikma riski
    - Kritik altyapilara saldiriyla, ülkenin felç edilmesi
    - Stuxnet, Estonia
  - Silahli saldiri boyutunda bir varsa, gerekli ve orantili (necessity and Proportionality Test) bir karşilik verilebilir.

# 2- Silahli Saldiri Sinir Aşan Boyutta Olmali

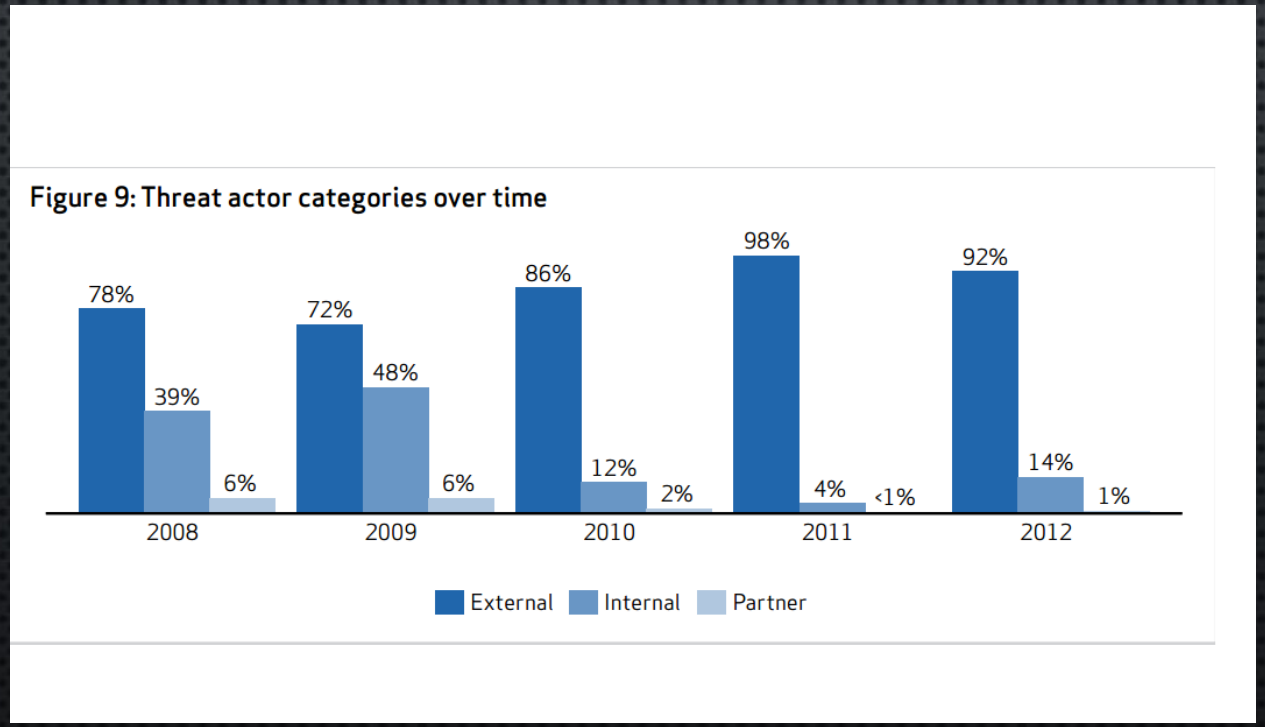
- Devlet – devlete
- Devlet – Devlet Dişi Aktör



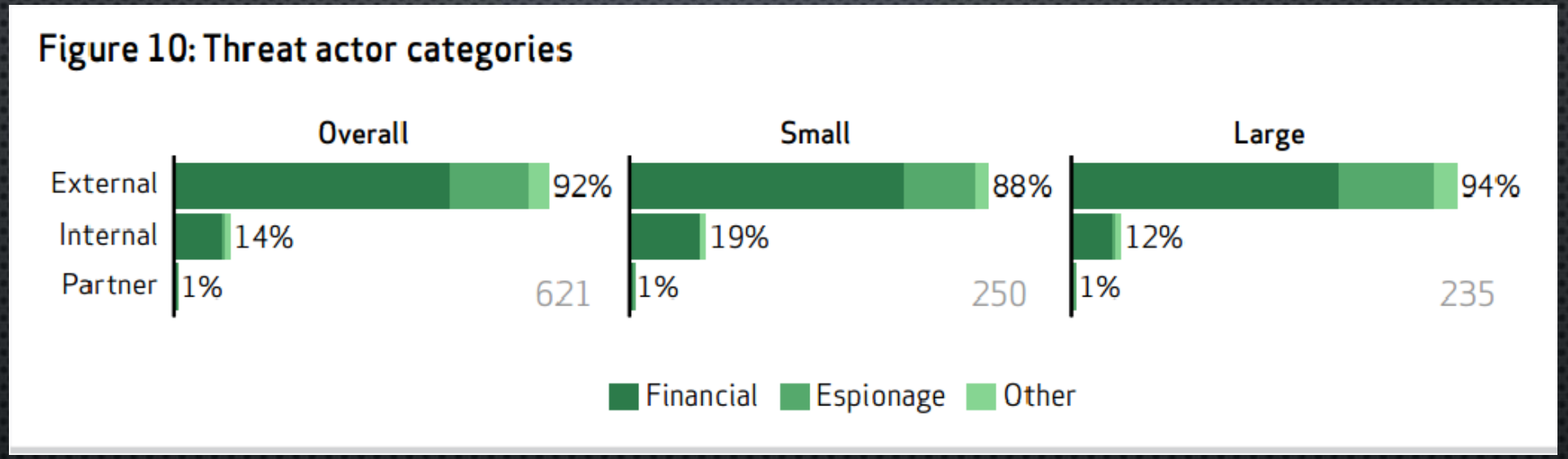
  - Peki

- Devlet dişi aktörlerin birbirine saldirmasi
- Şirketlerin birbirine saldirmasi Durumunda
  - Meşru Müdafaa?

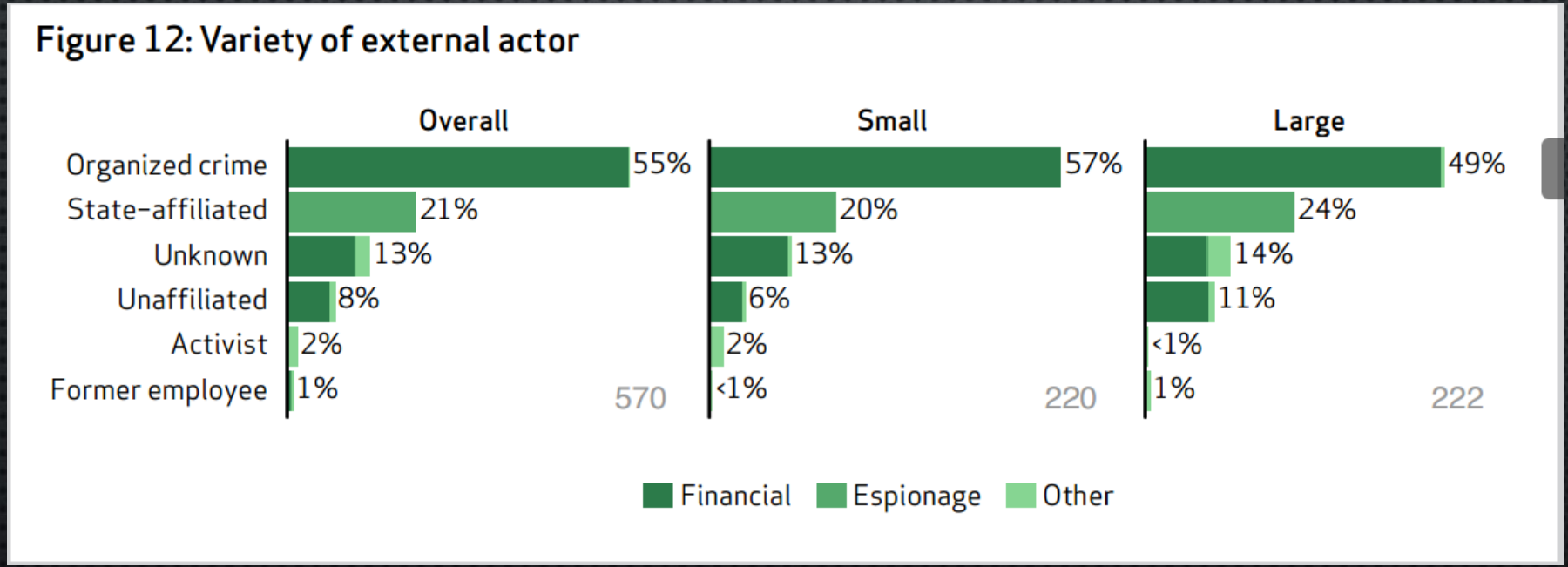
- VERİZON 2013 DATA BREACH INVESTİGATİONS REPORT:
  - 19 ULUSLARARASI KURULUŞ, 47.000 GÜVENLİK OLAYI, 621DOĞRULANMIŞ VERİ KAYBI
  - SALDIRILARIN %92'Sİ DIŞARIDAN,



- SALDIRILARIN BÜYÜK ÇOĞUNLUĞUNDAN FİNANSAL MOTİVASYON VAR.



- Saldırıların az bir oranı devlet destekli aktörler tarafından gerçekleştiriliyor. Motivasyon ise siber istihbarat.



- Devlet Dışı aktörlerin siber alanda devletlerden daha aktif ve etkili olduğu görülüyor.

- Saldırıları önlemek ve engellemek amacıyla Aktif Siber Savunma uygulamaları
  - Bal Çanağı (Honeypot): saldırını şaşırtma, hakkında bilgi toplama, saldırıyı önceden sonlandırma
  - Sistem için yapılar: Hangi dosyalar hedefte, hangi veriler aranıyor
  - Sistem dışı yapılar: Saldırı nereden geliyor, kaynağa erişim, saldıranın bilgisayarına giriş ve bilgisayarı tarama, yazılım yükleme, veri silme, değiştirme, çalışma

- TCK Bilişim Suçları Kapsaminda
- Uluslararasi bir saldiri var
  - Google, Siber saldiriya karşilik vererek, Tayvan'da bir bilgisayara erişim sağladi.
  - Ulaştiği veriler sadece kendi verileri değildi.
- Burada Şirketler Meşru Müdafaa kullanabilir mi? Kendi verilerini kurtarabilir, karşi tarafa saldirabilir mi? Hack-Back, Ön-Alici Hack?

- Zımnî Rıza
  - Diğer ülkenin kanunları
  - Gizliğin ihlali
- Self-Help
  - United States v. Alvarez-Machain (1992)
    - Cinayet şüphelisinin Meksika'dan kaçırılması
    - Supreme Court: Değişim anlaşması bulunmuyor, adaleti sağlanması için hukuka uygundur.
    - Güçlünün hukuku ?
  - Saldıranın tespit edilmesi ve adalete teslim edilmesi için zarar verici olmayan adımlar

# Sonuç

- Siber saldırılara devlet ağları nadiren maruz kalıyor.
- Silahlı saldırı boyutunda saldırı sadece bir ihtimal
  - Stuxnet ve Estonia
- Şirketler için büyük riskler söz konusu
- Zarar verici olmayan ama bilgi toplama ve kaynağı, sorumluları tespite yönelik adımlar hukuk mantığına uygun

# TEŞEKKÜRLER

OUZPEHLİVAN@GMAIL.COM