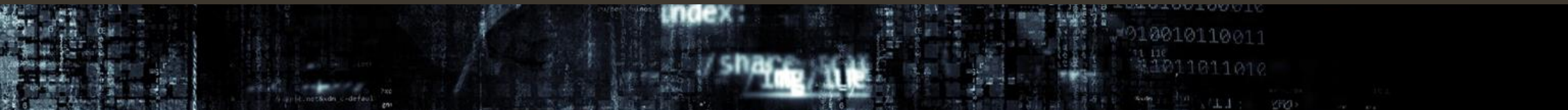
CYBERTERRORYZM

Artur J. Dubiel

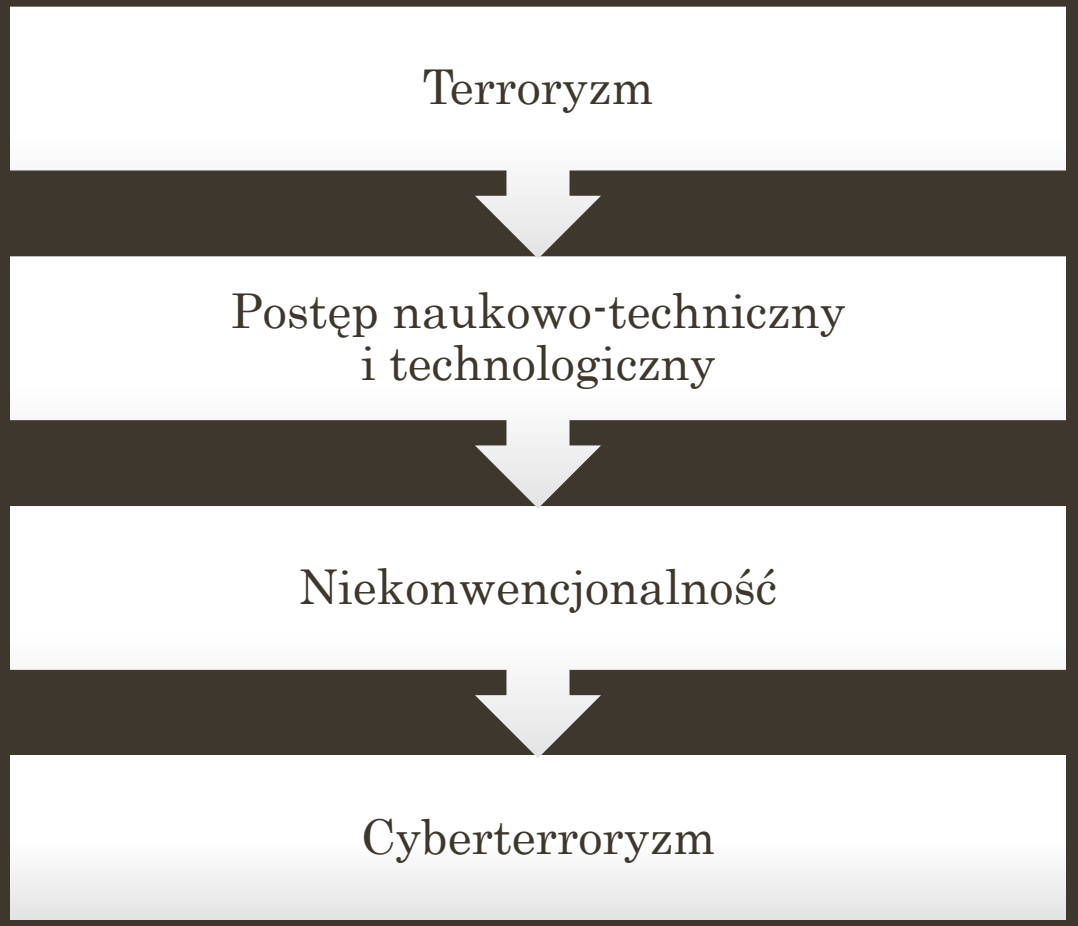


Bibliografia

- B. HOŁYST – Terroryzm (tom I)
- T. ALEKSANDROWICZ – Terroryzm międzynarodowy
- A. ŻEBROWSKI – Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego
- A. NOWAKOWSKA - KRYSTMAN i in. – Terroryzm w ujęciu analiz strategicznych
- P. BĄCZEK – Zagrożenia informacyjne a bezpieczeństwo państwa polskiego
- K. LIEDEL – Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego
- K. LIEDEL., S. MOCEK (red.) – Terroryzm w medialnym obrazie świata

TERRORYM A CYBERTERRORYZM

- przestępczość zorganizowana, w tym cyberprzestępczość powiązana z przestępczością ekonomiczną
- techniki telekomunikacyjne
- oddziaływanie na przeciwnika
- cyberprzestrzeń jako 5. obszar konfrontacji



Terminologia

- pierwszy raz termin *cyberterroryzm* został użyty w 1979 roku w raporcie Szwedzkiego Ministerstwa Obrony
- zawarto pierwsze rekomendacje dotyczące monitorowania

C Y B E R T E R R O R Y Z M

- ❖ infoterroryzm
- ❖ terroryzm informatyczny
- ❖ terroryzm sieciowy

(Żebrowski)

WSPÓŁCZESNY TERRORYZM
terroryzm klasyczny
superterroryzm (terroryzm ABC)
cyberterroryzm

E-DŻIHAD – DŻIHAD ELEKTRONICZNY

- początek XXI w. - komórki „dżihadu elektronicznego”
- zniszczenie witryn amerykańskich, izraelskich i innych „niewłaściwych”
- zadanie ekonomicznego ciosu, osłabienie morale
- paraliż sieci
- dni elektronicznego i cyfrowego dżihadu
- ataki DOS, spam, wirusy

(Liedel, Mocek)

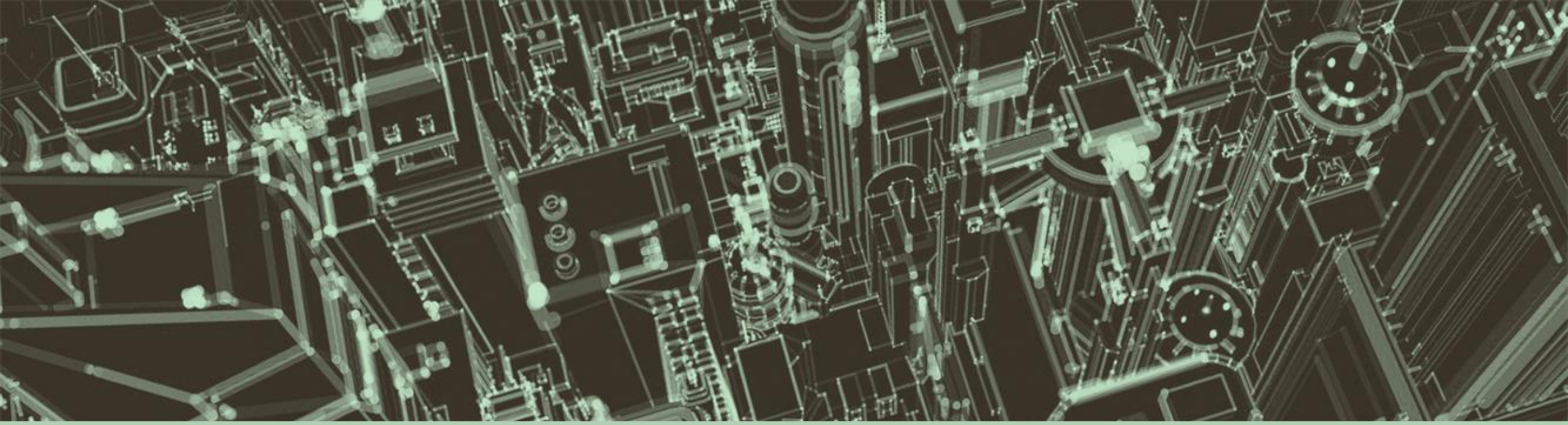
CYBERTERRORYZM

- przemyślany politycznie lub militarnie motywowany atak albo groźba ataku na systemy teleinformatyczne i teleinformacyjne oraz zgromadzone dane w celu sparaliżowania lub poważnego zniszczenia infrastruktury krytycznej państwa oraz zastraszenia i wymuszenia na rządzie lub społeczności daleko idących polityczno – militarnych działań
- świadome wykorzystanie systemów teleinformatycznych oraz globalnej sieci Internet przez organizacje terrorystyczne do propagandy, rekrutacji, mobilizacji, zbierania informacji o potencjalnych celach ataku, planowania i koordynacji akcji oraz szeroko pojętej dezinformacji i walki psychologicznej

(Lichocki)

CYBERTERRORYZM (Lichocki)

- bezpieczeństwo teleinformatyczne
- bezpieczeństwo teleinformacyjne
- technologie teleinformatyczne
- technologie teleinformacyjne
- bezpieczeństwo osobowe
- bezpieczeństwo fizyczne
- bezpieczeństwo danych osobowych
- prawo międzynarodowe
- prawo krajowe



STRATEGIA CYBERBEZPIECZEŃSTWA RP

NA LATA 2017 - 2022

STRATEGIA CYBERBEZPIECZEŃSTWA RP NA LATA 2017-2022

- Rozdział 6. Cel szczegółowy 2 – Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom
- Podrozdział 6.1 Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, występującej w cyberprzestrzeni

STRATEGIA CYBERBEZPIECZEŃSTWA RP NA LATA 2017-2022 (6.1)

W zakresie zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze terrorystycznym oraz działań o charakterze hybrydowym, ważne jest zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich ich fazach. Wymagana jest współpraca oraz koordynacja działań organów ścigania niezależnie od motywów, którymi kierują się sprawcy przestępstw. Istotne znaczenie ma zabezpieczenie dowodów elektronicznych.

STRATEGIA CYBERBEZPIECZEŃSTWA RP NA LATA 2017-2022 (6.1)

Zwiększenie efektywności czynności procesowych lub operacyjnych wymaga także poszerzenia współdziałania organów ścigania z innymi podmiotami, które mogą posiadać wiedzę w zakresie ustalenia istoty przestępstwa lub mogą przyczynić się do ustalenia jego sprawcy. Dotyczy to współpracy z krajowymi oraz międzynarodowymi podmiotami prywatnymi, szczególnie z sektora telekomunikacyjnego, bankowego oraz ubezpieczeniowego. Niezbędne jest zaangażowanie przedstawicieli organów ścigania, w tym Policji, w prace krajowych oraz międzynarodowych forów wymiany informacji o zagrożeniach i podatnościach.

STRATEGIA CYBERBEZPIECZEŃSTWA RP NA LATA 2017-2022 (6.1)

Mając na uwadze specyfikę cyberprzestrzeni zwalczanie cyberprzestępczości wymaga transgranicznej współpracy organów ścigania oraz podmiotów typu CERT/CSIRT. W czynnościach procesowych lub w procesie rozpoznania operacyjnego dotyczących przestępstw dokonywanych w cyberprzestrzeni krytyczny jest upływ czasu. Oznacza to, że wymagane są sprawne i zaufane kanały wymiany informacji pomiędzy organami ścigania różnych państw.

STRATEGIA CYBERBEZPIECZEŃSTWA RP NA LATA 2017-2022 (6.1)

Szybko zmieniające się metody popełniania przestępstw wymagają rozwijania badań naukowych w obszarze zwalczania cyberprzestępczości, których wyniki zapewnią wsparcie dla organów ścigania. Wyniki tych badań będą wykorzystywane w pracy organów ścigania i wymiaru sprawiedliwości, jak też będą stanowić materiał do opracowania działań profilaktycznych. Wdrożone zostaną, skierowane do społeczeństwa, programy informacyjne o zagrożeniach cyberprzestępczością oraz metodach unikania skutków tych zagrożeń. Wskazane zostaną sposoby postępowania dla osób dotkniętych przestępstwem. Ważną rolę do odegrania w tego typu działalności będą mieli operatorzy usług kluczowych, dostawcy usług cyfrowych, dostawcy usługi dostępu do Internetu oraz organizacje pozarządowe.