життя ділиться на до і після, людина змінюється і здебільшого в гіршу сторону більшості важко побороти психологічний бар'єр, який повстав перед нею і вона само знищується, як особистість.

Надзвичайно великий психологічний слід залишила Чорнобильська катастрофа після себе. Для багатьох українців катастрофа залишила величезні психологічні дірки, які дуже складно залатати. Радянська влада не замислювалася над тим, що буде з людьми, приховувавши від них правду, поширювавши дезінформацію. Приховання правди і обман це дуже великий удар по довірі, яка на довгі роки закарбується в свідомості людей. Відсутність довіри порушує цілісність людських взаємовідносин і відокремлює людину від соціуму, що в майбутньому призводить до плачевних наслідків.

Брак інформації і неправильна його подача в роки аварії, теж посприяла погіршенню взаємовідносин між людьми, оскільки на переселенців навісили ярлики " чорнобильців " і люди замість підтримки остерігалися тих людей.

Люди переїхавши з зони відчуження опинилися також в зоні відчуження від решти суспільства.

Надзвичайні ситуації і катастрофи трапляються за життя кожного покоління. І головне завдання керуючої влади і суспільства допомогти один одному пережити їх, як фізично так і психологічно. І надійним мостом який з'єднуватиме суспільство повинна стати надійна і правдива комунікація, оскільки людина боїться всього невідомого і нехватка інформацію може породжувати страх, який в свою чергу може завдати набагато більшої шкоди, ніж сама проблема.

В історії українців було багато випробувань, історія навчає на помилках, тому варто пам'ятати помилки минулого і потрібно зробити все те, щоб не повторювати їх в майбутньому.

**Література**

1. https://uk.wikipedia.org/wiki/%D0%A7%D0%BE%D1%80%D0%BD%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D1%81%D1%8C%D0%BA%D0%B0_%D0%BA%D0%B0%D1%82%D0%B0%D1%81%D1%82%D1%80%D0%BE%D1%84%D0%B0
2. https://suprun.doctor/kultura/pro-psixologichni-naslidki-chornobilskoyi-katastrofi.html?=page1250
3. https://zp.edu.ua/sites/default/files/konf/tema_4_konspektu_lekciy_zmistovogo_modulyu_no1_bzhd_proyekt_petryshchev.pdf
4. Зацарний В.В.,Зацарна О.В., Землянська О.В., Праховнік Н.А. Безпека життєдіяльності. Навчальний посібник. – Київ, НТУУ «КПІ», 2016.
5. https://gurt.org.ua/articles/32191/

## Секція 3. ГІБРИДНІ ВІЙНИ: ІСТОРИЧНІ ТА ПСИХОЛОГІЧНІ АСПЕКТИ

**Materniak D., Dr. nauk o bezpieczeństwie**
Portal Polsko-Ukraiński polukr.net, Polska

### ZAGROŻENIA HYBRYDOWE A AWARIE TECHNOLOGICZNE: RYZYKA I ŚRODKI REAGOWANIA

**Materniak D., Ph.D.**

# HYBRID THREATS AND TECHNOLOGICAL DISASTERS: RISKS AND RESPONSE MEASURES

## 1. Wojna hybrydowa: definicja zjawiska.

Choć konflikt zbrojny o charakterze określanym jako „wojna hybrydowa" nie jest nowym „wynalazkiem", to należy przyznać, że pojęcie to w aktualnym znaczeniu zrobiło karierę stosunkowo niedawno, bo na początku XXI wieku. W krajach Europy Środkowo-Wschodniej termin ten jest jednoznacznie kojarzony z działaniami Federacji Rosyjskiej wobec Ukrainy, trwającymi od przełomu 2013 i 2014 roku, efektem których była aneksja Krymu oraz początek wojny na wschodzie Ukrainy.

Samo określenie „wojna hybrydowa" poprzez wyróżniający go przymiotnik „hybrydowy" sugeruje, że jest to konflikt zbrojny o dużym zasięgu i znacznych konsekwencjach, którego specyfika polega na łączeniu w sobie cech różnych typów konfliktów zbrojnych. W odniesieniu do współczesnych konfliktów zbrojnych podkreślana tym samym „hybrydyzacja konfliktów zbrojnych" może być rozumiana jako równoległe współistnienie elementów „starych" i „nowych" wojen, klasycznych konfliktów zbrojnych i wojen „ponowoczesnych", starcia narodowych armii i konfliktów asymetrycznych, zaawansowanych technologii wojskowych i równocześnie prymitywnych broni, walki o terytoria i zasoby oraz sporów o tożsamość i wartości. „Hybrydyzacja" może dotyczyć zarówno podmiotu biorącego udział w wojnie, jak i środowiska, w jakim toczy się walka, oraz stosowanych metod i natury konfliktu[1]. Termin ten pojawia się m.in. w literaturze amerykańskiej dla opisania charakteru konfliktu zbrojnego pomiędzy Izraelem a Hezbollahem (m.in. w kontekście wojny z 2006 roku), gdzie zwrócono uwagę na stracie dwóch sił stosujących regularne i nieregularne metody walki[2].

Jak zostało wspomniane wyżej, w kontekście działań zbrojnych na Krymie i w Donbasie bardzo często pojawia się określenie „wojna hybrydowa". W ocenie dr Artura Gruszczaka, który porusza tę problematykę w opracowaniu „Hybrydowość współczesnych wojen – analiza krytyczna", koncepcja „wojen hybrydowych" powstała w USA jako próba wyjaśnienia przyczyn niepowodzeń silniejszych armii w wojnie ze słabszym przeciwnikiem prowadzonych na określonym, poddanym kontroli terytorium (m.in. w Iraku i Afganistanie), gdzie ewidentny sukces militarny w operacji wojskowej, zmierzającej do zajęcia tego terytorium, nie oznaczał zarazem osiągnięcia założonych, długofalowych celów w płaszczyźnie politycznej i społecznej[3]. Wobec powyższego, określenie to, przynajmniej w jego klasycznym i oryginalnym znaczeniu, niespecjalnie pasuje do sytuacji, z jaką mamy do czynienia na wschodzie Ukrainy, zwłaszcza że w miarę upływu czasu i postępującej eskalacji konfliktu coraz bardziej zaczyna on przypominać klasyczny konflikt zbrojny. Pomijając jednak oryginalne znaczenie tego terminu, warto zauważyć, że definicje wojen hybrydowych zdecydowanie lepiej opisują konflikt w Donbasie – zwłaszcza jego początkową fazę (a także w dużej mierze przebieg aneksji Krymu). Chodzi tu przede wszystkim o zastosowanie przez Rosję jednostek specnazu, grup dywersyjnych, formacji złożonych z najemników, itp. w charakterze trudnych do identyfikacji „zielonych ludzików". W tym kontekście warto także zwrócić uwagę na podejście amerykańskiego politologa Franka Hoffmana, który opisuje zjawisko hybrydowości wojen jako integrację konwencjonalnego użycia siły, taktyk walki nieregularnej, terroryzmu i podobnych zjawisk dla osiągnięcia określonego celu politycznego[4].

---

[1] A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, Biuro Bezpieczeństwa Narodowego, Warszawa 2011, s. 11.
[2] M. Banasik, *How to understand a hybrid war*, "Securitologia", No 1/2015, s. 19-20.
[3] A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, dz. cyt., s. 10.
[4] F. Hoffman, D. Kilcullen, za: M. Banasik, *How to understand a hybrid war*, dz.cyt. s. 24.

## 2. Infrastruktura krytyczna, zakłady przemysłowe i ryzyka związane z ich funkcjonowaniem.

Infrastruktura krytyczna to termin używany w odniesieniu do zasobów mających podstawowe znaczenie dla funkcjonowania społeczeństwa i gospodarki. Są to m.in. instalacje, urządzenia i obiekty służące do:
- produkcji, przesyłania i dystrybucji energii elektrycznej (energetyka);
- produkcji, transportu i dystrybucji paliw gazowych
- produkcji, transportu i dystrybucji ropy naftowej i produktów ropopochodnych;
- telekomunikacji (komunikacji elektronicznej);
- gospodarki wodnej (woda pitna, ścieki, wody powierzchniowe);
- do produkcji i dystrybucji żywności;
- do ogrzewania (składy paliw, elektrociepłownie);
- ochrony zdrowia (szpitale, ośrodki zdrowia, itp.);
- transportu (drogi, kolej, lotniska, porty);
- instytucji finansowych (banki);
- służb bezpieczeństwa (policja, wojsko, ratownictwo).

W Dyrektywie UE z 2008r. stwierdzono, że „infrastruktura krytyczna" oznacza składnik, system lub część infrastruktury zlokalizowanej na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji[5].

Szczególne znaczenie jeśli chodzi o zagrożenia awariami technologicznymi mają zakłady przemysłowe które wykorzystują w ramach swojej codziennej pracy substancje lub sposoby produkcji, które, w przypadku awarii – o charakterze naturalnym lub antropogenicznym – stwarzają poważne ryzyka dla życia i zdrowia ludzi, zarówno pracowników jak i osób zamieszkujących w pobliżu takich zakładów. W polskim ustawodawstwie kwestie te regulowane są w odpowiedniej ustawie, gdzie wymienia się w zależności od rodzaju, kategorii i ilości substancji niebezpiecznych Zakłady Zwiększonego Ryzyka (ZZR) oraz Zakłady Dużego Ryzyka (ZDR) wystąpienia awarii przemysłowych. O tym, czy zakład zostanie zaliczony do kategorii ZZR czy ZDR decyduje minister gospodarki w odpowiednim rozporządzeniu, w porozumieniu z ministrem zdrowia, spraw wewnętrznych i administracji oraz ochrony środowiska. Do substancji szczególnie niebezpiecznych zalicza się materiały: toksyczne, bardzo toksyczne, utleniające, wybuchowe, łatwopalne, wysoce łatwopalne, skrajnie łatwopalne oraz szczególnie niebezpieczne dla ludzi i środowiska[6]. Ustawa wprowadza także definicję poważnej awarii przemysłowej. W jej rozumieniu jest to zdarzenie, w szczególności emisja, pożar lub eksplozja, powstałe w zakładzie w trakcie procesu przemysłowego, magazynowania lub transportu, w których występuje jedna lub więcej niebezpiecznych substancji, prowadzące do natychmiastowego powstania zagrożenia życia lub zdrowia ludzi lub środowiska lub powstania takiego zagrożenia z opóźnieniem[7]. Według danych i przepisów z 2010 w Polsce liczba zakładów posiadających podobny status

[5] https://rcb.gov.pl/infrastruktura-krytyczna/, dostęp: 14.04.2021r.
[6] Ustawa Prawo ochrony środowiska: z dnia 27 kwietnia 2001 roku (Dz. U. 2001 Nr 62 poz. 627), a w szczególności Tytuł IV: Poważne awarie.
[7] Ustawa Prawo ochrony środowiska: z dnia 27 kwietnia 2001 roku (Dz. U. 2001 Nr 62 poz. 627.

to około 1200 obiektów w skali całego kraju[8]. Z kolei zgodnie z nowszymi regulacjami i danymi z 2015 roku liczba ta wyniosła 408 (stan na 31 grudnia 2015r.)[9].

Najtragiczniejsza katastrofa tego rodzaju miała miejsce w 1984 roku w indyjskim mieście Bhopal. W wyniku wycieku ponad 40 ton izocyjanianu metylu z fabryki pestycydów (będącej własnością amerykańskiej firmy Union Carbide) zmarło ok. 15 tysięcy osób, znaczna liczba ludzi doznała poważnego uszczerbku na zdrowiu, a ponad pół miliona mieszkańców miało kontakt z niebezpieczną substancją. Awarie w zakładach przemysłowych zdarzały się również w Europie: w 1976 w mieście Seveso w północnych Włoszech, w zakładach produkujących nawozy sztuczne doszło do eksplozji, w wyniku której doszło do skażenia środowiska (atmosfery, powierzchni ziemi oraz wód powierzchniowych i gruntowych) znaczną ilością substancji toksycznych i rakotwórczych. W wyniku tej katastrofy poszkodowanych zostało ponad 2000 osób. Między innymi dlatego problematyka awarii przemysłowych została uznana za istotną na tyle, iż powinna być uregulowana osobnymi przepisami na szczeblu całej Unii Europejskiej. Pierwszym tego typu uregulowaniem była dyrektywa Europejskiej Wspólnoty Gospodarczej nr 82/501/EWG z 24 czerwca 1982 roku, w sprawie zagrożenia poważnymi awariami przez niektóre rodzaje działalności przemysłowej, znana także jako Dyrektywa Seveso. Jej nowelizacją jest przyjęta 9 grudnia 1996 roku dyrektywa Seveso II: dyrektywa Rady Unii Europejskiej 96/82/EC dotycząca zarządzania poważnymi awariami przemysłowymi z udziałem substancji niebezpiecznych, oraz będąca jej uzupełnieniem Dyrektywa 2003/105/WE[10]. W 2015 roku miała miejsce zmiana przepisów w ramach kolejnej dyrektywy funkcjonującej jako Seveso III[11].

## 3. Zagrożenia militarne a zakłady przemysłowe: potencjalne ryzyka i możliwości reagowania.

Ochrona infrastruktury krytycznej to wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Zagrożenia, które bardzo często wywołują sytuacje kryzysowe, mają wpływ na bezpieczeństwo i prawidłowe funkcjonowanie całego państwa, można podzielić na poszczególne kategorie:

- zagrożenia naturalne (powodzie, silne wiatry, susze, ruchy tektoniczne, itp.),
- zagrożenia techniczne (wynikające z problemów, błędów, awarii i podobnych przyczyn powodujących zakłócenia w funkcjonowaniu obiektów w ramach infrastruktury krytycznej),
- terroryzm i konsekwencje działań zbrojnych.

Ten ostatni element jest szczególnie znaczący z punktu widzenia zagrożeń związanych z konfliktami o charakterze hybrydowym. To właśnie obiekty infrastruktury krytycznej są i zapewne będą w przyszłości obiektami działania podmiotów, które są zaangażowane w działania o charakterze hybrydowym.

[8]https://m.ciop.pl/CIOPPortalWAR/appmanager/ciop/mobi?_nfpb=true&_pageLabel=P42600613191498038218695&html_tresc_root_id=300007540&html_tresc_id=300007646&html_klucz=300007540&html_klucz_spis= (dostęp: 15.04.2021r.).

[9]https://m.ciop.pl/CIOPPortalWAR/appmanager/ciop/mobi?_nfpb=true&_pageLabel=P42600613191498038218695&html_tresc_root_id=300007540&html_tresc_id=300007542&html_klucz=300007540&html_klucz_spis= (dostęp: 15.04.2021r.).

[10] Dyrektywa Seveso II; dyrektywa Rady Unii Europejskiej 96/82/EC.

[11]https://www.ciop.pl/CIOPPortalWAR/appmanager/ciop/pl?_nfpb=true&_pageLabel=P1500015622134692594558&html_tresc_root_id=25314&html_tresc_id=300002010&html_klucz=25314&html_klucz_spis=25314 (dostęp: 15.04.2021r.).

„Czerwone światła ostrzegawcze migały na każdym z czterech wysokich kominów elektrowni, dając ludziom w dwóch samochodach niezawodną pomoc w nawigacji. Nawet gdyby zgasły, i tak drogę znali na pamięć. Jechali szybko, jak na radiowozy na sygnale przystało, zwłaszcza o trzeciej w nocy na pustej leśnej drodze. Kapitan Dymitr Kardaszew z 45 Brygady Specjalnego Przeznaczenia Wojsk Powietrznodesantowych, widząc światła bramy, przeładował broń. Upewnił się, że przyczepione rzepami do munduru emblematy są na miejscu. Od nich zależało powodzenie całego planu. Byli uzbrojeni prawie tak, jak estoński oddział antyterrorystyczny (...) Elektrownia Esti, czyli po prostu „Estonia", podobnie jak druga bliźniacza instalacja w rejonie Narwy, jest elektrownią cieplną, spalającą ropę wydobywaną z miejscowych złóż łupkowych. Jej działanie zapewnia woda pobierana z pobliskiej rzeki. Aby ją unieruchomić, nie trzeba niszczyć całego zakładu ani nawet ogromnych kotłów i turbin służących do produkcji prądu. Po obezwładnieniu operatorów pomp założyli na maszynach precyzyjne, małe ładunki wybuchowe. Eksplozje nie były duże ani bardzo głośne (...) Estonia utraciła siedemdziesiąt pięć procent energii. Ludzie, którzy wstali rano, nie mogli zapalić światła. Tramwaje i trolejbusy w Tallinie nie wyjechały na ulice. Nie działały bankomaty ani terminale płatnicze. Sieci komórkowe funkcjonowały z przerwami, aż w końcu wyłączono je, gwarantując łączność tylko dla służb państwowych (...) Ci, którzy mieli dostęp do Internetu, mogli przeczytać lakoniczny komunikat: W akcie słusznego protestu przeciwko niszczeniu środowiska naturalnego, Europejski Front Oporu przeprowadził akcję bezpośrednią przeciwko utrzymywanym przez estoński, nacjonalistyczny rząd elektrowniom"[12].

Zacytowany fragment jest częścią powieści z gatunku fikcji polityczno-militarnej. Trudno jednak odmówić racji autorowi tego i podobnych scenariuszy, pojawiających się przecież nie tylko w literaturze rozrywkowej, ale również w analizach i prognozach ośrodków analitycznych, a także – w rzeczywistości. Odnosząc się do kwestii działań wymierzonych w infrastrukturę krytyczną wystarczy przywołać działania, które miały miejsce na Krymie i Donbasie w 2014 roku. W pierwszej fazie rosyjskiej agresji celami działania prorosyjskich bojowników, grup dywersyjnych i „zielonych ludzików" były obiekty administracji rządowej (np. siedziba parlamentu AR Krym w Symferopolu), siedziby sił bezpieczeństwa i służb specjalnych (np. siedziby Milicji, SBU czy jednostki wojskowej – na Krymie i Donbasie, np. w Słowiańsku), a także obiekty przemysłowe (kopalnie, zakłady produkcyjne, stacje pomp, itp.) czy infrastruktura transportowa (mosty, kluczowe skrzyżowania, itp.).

Prawdopodobieństwo wybuchu pełnoskalowej wojny w regionie jest stosunkowo niewielkie, nawet pomimo działań militarnych o charakterze zastraszania, jakie od wielu lat realizuje Rosja – pod pozorem manewrów wojskowych takich jak Zapad-17 czy Kaukaz-20. Zdecydowanie bardziej realnym scenariuszem są pośrednie formy stosowania przemocy zbrojnej: w postaci operacji dywersyjnych, zbliżonych do działań o charakterze terrorystycznym (choć należy tutaj wskazać istotną różnicę: o ile terrorystom zwykle chodzi o osiągnięcie swoich celów poprzez maksymalizację liczby ofiar, o tyle w przypadku działań hybrydowych celem zdecydowanie częściej jest przejęcie i utrzymanie kontroli nad danym obszarem czy obiektem, a niekoniecznie powodowanie strat w ludziach czy zniszczeń).

Należy oczekiwać, że w przypadku kolejnych konfliktów o charakterze hybrydowym w regionie Europy Środkowo-Wschodniej to właśnie obiekty infrastruktury krytycznej będą jednym z głównych celów działania „sił hybrydowych" i to nie jako cel sam w sobie – ale po to, by za ich pośrednictwem uzyskać kontrolę nad danym obszarem i zmusić mieszkańców do podejmowania takich czy innych działań (np. nacisku na władze dla wymuszenia określonych decyzji politycznych). Konsekwencje np. pozbawienia elektryczności i ogrzewania dużych grup ludności w środku sezonu zimowego byłyby nieobliczalne.

[12] A. Langer, *Wojna hybrydowa*, Wyd. Warbook, Ustroń 2018, s. 13-17.

W zależności od wyboru danej metodologii działania, awarie lub zniszczenia danych obiektów przemysłowych czy (szerszej) IK mogą być skutkiem ubocznym (np. na skutek przypadkowego ostrzelania) lub potencjalnym głównym celem działania „sił hybrydowych" (np. w formie zniszczenia lub groźby zniszczenia zakładu przemysłowego należącego do kategorii ZZR/ZDR).

Z punktu widzenia państwa jako całości, jak również administracji na poziomie lokalnym i regionalnym, konieczne jest posiadanie sił i środków pozwalających na reagowanie na pojawiające się zagrożenia o charakterze hybrydowym. Oznacza to przede wszystkim zdolności w dwóch głównych obszarach:

1) niedopuszczenie do sytuacji w której dochodzi do sytuacji zagrożenia ludności lub środowiska działaniami o charakterze hybrydowym. W tym obszarze konieczne jest posiadanie odpowiednio sprawnych służb odpowiedzialnych za bezpieczeństwo, tj. po pierwsze za wczesne ostrzeganie, wykrywanie i identyfikację zagrożeń (służby specjalne: wywiad i kontrwywiad) jak również odpowiedzialnych za adekwatne reagowanie w przypadku wystąpienia tych zagrożeń (siły policyjne i zdolne współpracować z nimi siły wojskowe, zwłaszcza posiadające odpowiednie zdolności do działań kontrterrorystycznych). W przypadku Polski są to, poza służbami specjalnymi (cywilnymi i wojskowymi) jednostki Policji, Straży Granicznej czy wyspecjalizowanych służb np. Straży Ochrony Kolei, jak również odpowiednie jednostki funkcjonujące w ramach Sił Zbrojnych RP.

2) posiadania zasobów, sił i środków pozwalających na maksymalne ograniczenie skutków przeprowadzenia takich działań w odniesieniu do obiektów IK, co sprawia, że próba szantażu takimi działaniami staje się nieskuteczna. Są to instytucje państwowe odpowiedzialne za ochronę życia, zdrowia oraz mienia i środowiska naturalnego. W Polsce za działania te odpowiadają jednostki skupione w ramach Krajowego Systemu Ratowniczo-Gaśniczego (KSRG), którego zadaniem jest prowadzenie działań mających na celu zwalczanie pożarów i innych klęsk żywiołowych, ratownictwo chemiczne, techniczne, ekologiczne oraz ratownictwo medyczne. W ramach KSRG funkcjonują m.in. jednostki Straży Pożarnej (Państwowej i Ochotniczej), jak również Zespoły Ratownictwa Medycznego (także w ramach organizacji ochotniczych, np. Polskiego Czerwonego Krzyża). W ostatnim czasie, zwłaszcza w związku z trwającą od marca 2020 roku pandemią koronawirusa SARS-Cov-2 istotnym wsparciem dla systemu KSRG (zwłaszcza dla placówek ochrony zdrowia, tj. szpitali) są jednostki Wojsk Obrony Terytorialnej, kierującej swój personel do odpowiednich działań wymagających zwiększonego zaangażowania personelu. Równie istotnym elementem który wymaga w Polsce dopracowania jest systemy Obrony Cywilnej, który istnieje praktycznie tylko „na papierze".

Aktualne wyzwania związane z trwającą pandemią Covid-19 są istotnym testem dla administracji i służb państwowych odpowiedzialnych za bezpieczeństwo obywateli. Sytuacja ta pozwala (siłą rzeczy) na sprawdzenie zdolności funkcjonowania poszczególnych instytucji w warunkach realnego kryzysu, momentami (w trakcie narastania kolejnych fal zachorowań) w warunkach zbliżonych niemal do wojennych (np. po względem zaangażowania personelu czy obciążenia placówek medycznych). To trudny test, ale jego efektem są i będą (a przynajmniej powinny być) także wnioski dotyczące możliwości usprawnienia funkcjonowania mechanizmów działania i współpracy poszczególnych służb jak i ich współdziałania. Doświadczenia te mogą okazać się bezcenne także z punktu widzenia przyszłych zagrożeń hybrydowych.

**Literatura**

1. M. Banasik, *How to understand a hybrid war*, "Securitologia", nr 1/2015.
2. J.R. Davis, *Continued evolution of hybrid threats*, „Theree Swords Magazine", 28/2015.

3. A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, Biuro Bezpieczeństwa Narodowego, Warszawa 2011.
4. A. Langer, *Wojna hybrydowa*, Wyd. Warbook, Ustroń 2018.
5. R. Porowski, *System zapobiegania poważnym awariom przemysłowym w Polsce*, www.straz.gov.pl.
6. A. Rękas, „Zapobieganie awariom przemysłowym", w: Magazyn *W akcji – technika, taktyka, profilaktyka*", nr 4/2009.
7. Ustawa Prawo ochrony środowiska: z dnia 27 kwietnia 2001 roku (Dz. U. 2001 Nr 62 poz. 627).
8. https://m.ciop.pl
9. https://www.rcb.gov.pl
10. https://www.strazgov.pl

**Weissmann M., Assoc. Prof. ; Nilsson N., Senior Lecturer; Palmertz B., Senior Analyst**
Swedish Defence University

## COMPREHENDING HYBRID THREATS AND HYBRID WARFARE: THE HYBRIDITY BLIZZARD MODEL[13]

**Authors:**
**Mikael Weissmann,** Associate Professor and the Head of Research and Deputy Head of the Land Operations Section at the Swedish Defence University, where he is also a co-convenor of the Hybrid Warfare Research Group (HWRG) and the Land Warfare Research Group (LWRG).
**Niklas Nilsson,** Senior Lecturer in War Studies at the Swedish Defence University, where he is also a co-convenor of the Hybrid Warfare Research Group (HWRG) and the Land Warfare Research Group (LWRG).
**Björn Palmertz,** senior analyst focusing on strategic communication and influence operations at the Center for Asymmetric Threat Studies (CATS), Swedish Defence University.

To fully comprehend and counter hybrid threats and hybrid warfare (HT&HW) is a complex task, but also a very important one. In this paper we will outline a schematic model for how to comprehend hybrid threats and hybrid warfare: the "Hybridity Blizzard Model". The model comes in three versions, of which the first presents a simplified picture of the dynamics of and between HT&HW, as well as responses and countermeasures. The second version adds a temporal dimension to this relationship, demonstrating how short term actions and responses relate to long-term vulnerabilities and resilience. The third version, in contrast, aims to provide a more accurate picture of the complex real-world situation. The aim of the model is to enable not only a better understanding of the dynamics themselves but also how to identify, comprehend and act against HT&HW .

The simplified Hybridity Blizzard Model outlines a schematic model of the dynamics of the interrelated relationship between defender and attacker in the short term as well as long term perspective, and how the different time and actor dimensions interact. The model depicts these interactive and temporal relationships as an ecosystem, which we believe is a good

[13] This paper is adopted from the authors conclusion of a volume on Hybrid Warfare: Weissmann, Mikael, Niklas Nilsson, and Björn Palmertz. "Moving out of the blizzard: Towards a comprehensive approach to hybrid threats and hybrid warfare." *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm . London: I.B. Tauris, 2021. 263–272. Download here: http://dx.doi.org/10.5040/9781788317795.0025. We would like to acknowledge support received from Riksbankens Jubileumsfond (RJ) (Grant No. F16-1240:1).