JOURNAL OF MODERN SCIENCE

6/60/2024

www.jomswsge.com

DOI: 10.13166/jms/199488

MACIEJ CIESIELSKI

WSGE University of Applied Sciences in Józefów, Poland

ORCID iD: 0000-0001-6868-884X

MOŻLIWOŚCI WYKORZYSTANIA SZTUCZNEJ INTELIGENCJI W ANALIZIE BEZPIECZEŃSTWA

POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE IN SECURITY ANALYSIS

Abstract

The aim of the article is to present the characteristics of analytical imagination appropriate for a scientist and practitioner working in the security domain. The text discusses a total of twelve features used in the security domain – five related to contextual thinking and seven related to critical thinking.

Abstrakt

Celem artykułu jest przybliżenie charakterystyki wyobraźni analitycznej właściwej dla naukowca i praktyka działającego w domenie bezpieczeństwa. W tekście omówiono łącznie jej dwanaście cech wykorzystywanych w domenie bezpieczeństwa – odpowiednio pięć dotyczących myślenia kontekstowego oraz siedem związanych z myśleniem krytycznym.

Keywords: *critical thinking, analytical imagination, contextual thinking, security analysis, artificial intelligence*

Słowa kluczowe: *myślenie krytyczne, wyobraźnia analityczna, myślenie kontekstowe, analiza bezpieczeństwa, sztuczna inteligencja*

Wstęp

Coraz częściej słyszy się rozważania na temat możliwości zmian na rynku pracy, jakie będą konsekwencją rozwoju sztucznej inteligencji (*Artificial Intelligence – AI*). W przestrzeni publicznej pojawiają się pytania o to, przedstawiciele których zawodów powinni się obawiać utraty pracy i przed którymi z nich jawi się konieczność przekwalifikowania.

Z drugiej strony, sztuczna inteligencja praktycznie zdominowała rozważania na temat kierunków rozwoju cyberprzestrzeni oraz charakteru relacji, jakie będą właściwe/specyficzne dla tej domeny. Cyberprzestrzeń i sztuczna inteligencja nie mają charakteru abstrakcyjnego. Na całym świecie powstają wojska obrony cyberprzestrzeni. Sztuczna inteligencja jest już na polu walki, wspiera żołnierzy w procesach decyzyjnych, ale przede wszystkim jest immanentnym elementem systemów uzbrojenia – które stopniowo ewoluują w stronę systemów autonomicznych *(Lethal Autonomous Weapons Systems – LAWS*).

Zakres relacji oraz charakter interakcji i komunikacji człowieka ze sztuczną inteligencją zmienia się. Cyberprzestrzeń jest polem walki, ale także sferą codziennych kontaktów aktorów społecznych. Rozwój technologii doprowadził do tego, że cyberprzestrzeń jest sferą relacji człowieka z systemami teleinformatycznymi (łącznie z ich oprogramowaniem) oraz z innymi ludźmi poprzez te systemy, a także samych systemów teleinformatycznych między sobą (zob. K. Chałubińska-Jankiewicz, 2019, s. 8-9). Jednak w przekazach społecznych sztuczna inteligencja pojawiła się jako wyodrębniony podmiot (grupa podmiotów?) posiadający nowe zdolności komunikacyjne i definiująca relacje społeczne w cyberprzestrzeni na nowo. Chodzi tutaj o ujęcie socjologiczne, a nie prawne. W przestrzeni komunikacyjnej, w ramach codziennych interakcji społecznych – w tym tych realizowanych przy wykorzystaniu mediów – doszło do upodmiotowienia sztucznej inteligencji (w świadomości społecznej). Na podstawie indywidualnych przekazów oraz tych pojawiających się w sferze publicznej, można postawić tezę, że AI jest traktowana jako odrębny byt. Pomimo że w świetle regulacji prawnych oraz w ujęciu technicznym (technologicznym), sztuczna inteligencja nadal mieści się w pojęciu definicji cyberprzestrzeni i relacji w niej zachodzących. Idzie zatem o budowanie konstruktów społecznych, wprowadzanie nowego aktora społecznego u ujęciu percepcji społecznej.

W takim socjologicznym (konstruktywistycznym) podejściu, cyberprzestrzeń nie byłaby już wyłącznie przestrzenią nawiązywania relacji i komunikacji [ponieważ to w praktyce oznacza wymiana informacji] pomiędzy ludźmi za pośrednictwem systemów teleinformatycznych, tych samych ludzi z systemami teleinformatycznymi (w tym z ich oprogramowaniem) czy pomiędzy systemami teleinformatycznymi. Chodzi o pojawienie się specyficznych interakcji ze sztuczną inteligencją. Specyfika ta ma jednak swoje źródło nie tyle we właściwościach cyberprzestrzeni, co w budowaniu wokół niej narracji przez społeczeństwo jako całości oraz poszczególne grupy społeczne (grupy interesu). Sposób działania algorytmów definiujących sztuczną inteligencję jest już właściwy dla aktorów społecznych. Strony interakcji nie potrafią od razu i jednoznacznie określić, kto jest partnerem interakcji – maszyna czy człowiek. To powoduje zmianę *opowieści* społecznej na temat cyberprzestrzeni i nadania nowego – odrębnego statusu – sztucznej inteligencji.

W powyższym kontekście kształtuje się nowy potencjał analityczny sztucznej inteligencji, który jest osadzony w zdolnościach komunikacyjnych oraz kształtowanych na ich podstawie normach postępowania. Chodzi konkretnie o definiowanie przez sztuczną inteligencją granic w oparciu o pierwotne ramy interakcji. W tym kontekście istotny jest zakres autonomicznego działania sztucznej inteligencji, który może się zmieniać ze względu na otwarty charakter algorytmu zakładającego uczenie się w toku interakcji z człowiekiem – ale także z innymi algorytmami. W niniejszym opracowaniu ważne jest wyodrębnienie sztucznej inteligencji jako istotnego aktora (aktorów) działającego w cyberprzestrzeni, którego pierwotny potencjał jest zakreślany przez człowieka, ale jednocześnie od człowieka – na kolejnych etapach interakcji – niezależnego w ramach procesów decyzyjnych. Należy podkreślić, że pomimo mówienia o *aktorach,* sztuczną inteligencję analitycy cały czas traktują jako odrębne narzędzie wpierające pracę analityczną i same procesy decyzyjne.

Powyższe możliwości sztucznej inteligencji należy osadzić w domenie bezpieczeństwa. Sferze rządzącej się swoimi prawami, właśnie ze względu na wyjątkowe nacechowanie emocjonalne i subiektywny aspekt fenomenu, który jest uwypuklony przede wszystkim w cyberprzestrzeni. Tak w kontekście identyfikowania jej jako przestrzeni komunikacyjnej, ale i możliwości oprogramowania zabezpieczającego systemy operacyjne – w tym uzbrojenia. Chodzi zatem o potraktowanie sztucznej inteligencji, w niniejszych rozważaniach, jako autonomicznego narzędzia analitycznego, które dopiero kształtuje swoje kompetencje w obszarze myślenia kontekstowego oraz myślenia krytycznego. Sfera bezpieczeństwa jest jeszcze trudniejsza do wykorzystania sztucznej inteligencji, ponieważ zawsze z takimi analizami powiązane jest identyfikowanie stanów obiektywnych na podstawie różnych linii narracyjnych przedstawianych przez liczne grupy interesu. Procesy te są jeszcze lepiej widoczne w cyberprzestrzeni, która w chwili obecnej jest podstawowym polem dezinformacji w dziedzinie bezpieczeństwa.

Na realne i praktyczne możliwości wykorzystania AI w analizach bezpieczeństwa wskazują chociażby działania wybranych spółek zajmujących się wykorzystaniem oprogramowania i sztucznej inteligencji w branży obronnej – w tym do przetwarzania danych wywiadowczych. Takie spółki jak Palantir Technologies Inc. inwestują w budowę infrastruktury potrzebnej

do zasilania i szkolenia algorytmów AI (G. Kubera, 2023; www.palantir.com). Zaliczają się do spółek cechujących się największym wzrostem wartości akcji i kapitalizacji. Sztuczna inteligencja nie jest więc abstrakcyjnym bytem w pośredni sposób odwołującym się do domeny bezpieczeństwa, ale jest wykorzystywana do opracowywania produktów bezpośrednio wspierających żołnierzy na polu walki, usprawniających zautomatyzowane systemy uzbrojenia, ale przede wszystkim wkroczyła w nowy obszar – wspieranie procesów decyzyjnych w podsystemie politycznym i wojskowym.

Celem artykułu jest przybliżenie charakterystyki i potencjału analitycznego sztucznej inteligencji w obszarze analizy bezpieczeństwa. Tekst ma charakter wprowadzający – nie daje, ani nie prezentuje jednoznacznych odpowiedzi wskazujących, czy sztuczna inteligencja jest w chwili obecnej w stanie, albo w przewidywalnej przyszłości będzie w stanie, zastąpić człowieka w roli analityka bezpieczeństwa. Zasadnym jest postawienie następujących pytań badawczych:

- *Jaka jest charakterystyka wyobraźni analitycznej identyfikowanej jako narzędzie, które mogłoby być wykorzystane przez sztuczną inteligencje w analizach bezpieczeństwa?*
- *W jakich okolicznościach sztuczna inteligencja jest w stanie uwzględnić charakterystykę cyklu wywiadowczego w generowanych odpowiedziach i opracowaniach?*
- *Które cechy właściwe dla myślenia kontekstowego oraz myślenia krytycznego stanowią wyzwanie dla sztucznej inteligencji, a które są polem jej przewagi poznawczej nad człowiekiem?*

Wyobraźnia analityczna – potencjalne instrumentarium sztucznej inteligencji w analizie bezpieczeństwa

Pojęcie wyobraźni analitycznej wywodzę z dwóch źródeł. Po pierwsze, co nasuwa się na pierwszy rzut oka, jest to nawiązanie do *wyobraźni socjologicznej,* czyli pojęcia i koncepcji wprowadzonej przez Charles'a W. Millsa, rozumianej jako pewna kompetencja typowa dla badacza społecznego, ale przede wszystkim dla świadomego procesów społecznych obywatela. Wyobraźnia socjologiczna pozwala bowiem *zrozumieć historię i biografię oraz relację zachodzącą między nimi w ramach społeczeństwa* (Mills, 2008, s.53).

Drugie źródło to pojmowanie bezpieczeństwa jako procesu społecznego (Piwowarski, 2017, s. 17; Ciesielski, 2024, s. 286), czyli fenomenu dynamicznego, zmiennego, płynnego, który wymaga od analityka konkretnych narzędzi. Zwłaszcza pojmowania bezpieczeństwa jako wypadkowej wzajemnego oddziaływania i relacji pomiędzy jego komponentami (sektorami/płaszczyznami) obiektywnym i subiektywnym (Ciesielski, 2019, s. 131). Przy tym, w prowadzonych analizach należy uwzględnić *złożoność* jako cechę otoczenia, w którym wiele procesów i zdarzeń oddziałuje na siebie w domenie bezpieczeństwa w tym samym czasie. Bezpieczeństwo jest głęboko osadzone w sferze wartości i operacjonalizujących je interesów, co w istotnym zakresie osadza je w systemie prawnym – rozumianym także jako zbiór norm postępowania, które mają charakter wyraźnie sankcjonowany (pomimo braku w polskim systemie prawa definicji legalnej bezpieczeństwa).

Powyższe dwa źródła wyobraźni analitycznej wymagają kluczowego komponentu właściwego przede wszystkim dla umysłu ludzkiego, czyli świadomości. To właśnie świadomość rozumiana jako *zdawanie sobie sprawy z czegoś* (Słownik Języka Polskiego PWN) jest kluczowa.

Wyobraźnia analityczna składa się z dwóch wzajemnie warunkujących się oraz częściowo nachodzących na siebie elementów: myślenia kontekstowego oraz myślenia krytycznego. Oba te pojęcia mają swoje konkretne właściwości ze względu na specyfikę domeny bezpieczeństwa, na których skoncentruję się poniżej. Nie są tożsame, ponieważ odwołują się do odrębnych schematów postępowania związanych ze świadomością, ale są na tyle

komplementarne i ściśle ze sobą powiązane, że w pewnych obszarach mogą być traktowane niemalże zamiennie.

Specyfika myślenia kontekstowego w domenie bezpieczeństwa – obszar aktywności sztucznej inteligencji

Mówiąc o myśleniu kontekstowym, inaczej ramowaniu, mówimy o opracowywaniu produktów i prowadzeniu analiz przy zachowaniu odpowiedniej świadomości (M. Chrost, 2021). Niektórzy wskazują, że *sztuczna inteligencja podejmuje lepsze decyzje niż my i przejmuje nasze miejsca pracy, jednak komputery i algorytmy nie potrafią tworzyć i używać ram* (K. Cukier, V. Mayer-Schönberger, F. de Véricourt, 2022, s. 33). Dalej przywołani autorzy podkreślają, że sztuczna inteligencja nie ma sobie równych jeżeli chodzi o odpowiadanie na pytania zadawane przez ludzi, ale to właśnie ludzie dokonując ramowania zadają pytania, które nigdy nie były wcześniej sformułowane (s. 34).

Niniejszy tekst koncentruje się nie tylko na potencjale analitycznym sztucznej inteligencji (definiowanym poprzez możliwość wykorzystania wyobraźni analitycznej), ale na jego konkretnym wykorzystaniu w obszarze analiz bezpieczeństwa. Myślenie kontekstowe w tym zakresie musi uwzględniać występowanie następujących zmiennych wpływających na ostateczny kształt i wiarygodność produktu analitycznego (informacyjnego), a także relacji pomiędzy tymi zmiennymi. Chodzi o (1) charakterystykę źródeł informacji; (2) specyfikę zbierania danych/informacji; (3) błędy poznawcze na jakie jest narażony analityk; (4) procedury kodowania i dekodowania informacji z danych (*świadomość relacji: dane – informacje);* (5) wpływ czynników zewnętrznych na obniżenie wiarygodności informacji i analiz.

1. *Charakterystyka źródeł informacji* – dla jakości i trafności produktu analitycznego fundamentalna jest wiarygodność źródła pochodzenia informacji oraz możliwość weryfikowania danych w oparciu o inne źródła. W tym kontekście ważne jest także rozpoznawanie człowieka oraz AI jako źródeł informacji, które wpływają na jej zasięg oraz wagę. Wydaje się, że sztuczna inteligencja przynajmniej częściowo jest w stanie dokonać

takiej charakterystyki. W tym pod kątem szacowania wiarygodności informacji i ich źródeł. Jednak nie wydaje się, aby ta umiejętność była w pełni rozwinięta z uwagi na ograniczone możliwości krytycznego myślenia – drugiego kluczowego elementu wyobraźni analitycznej. W tym obszarze chodzi o konfrontację perspektyw i świadomość ich odrębności. Każde źródło informacji, zwłaszcza osobowe, reprezentuje jakieś interesy – własne lub zapożyczone – identyfikuje się z nimi, co często się *przebija* zwłaszcza do oceny informacji zaprezentowanej w materiale. W konsekwencji analityk bezpieczeństwa musi sobie zdawać sprawę z obciążeń płynących z charakteru i pochodzenia źródeł informacji. Dotyczy to nie tylko źródeł osobowych, ale także wszelkiego rodzaju opracowań/utworów pierwotnych autorów analiz i ocen informacji, w tym również przetworzonych w cyberprzestrzeni.

2. *Specyfika zbierania danych/informacji* – w tej zmiennej chodzi o ustalenie, w jaki sposób informacje zostały zebrane –przez człowieka lub w cyberprzestrzeni. Nie chodzi zatem tylko o samo przetwarzanie danych w cyberprzestrzeni, ale o to jak zostały zebrane przed wprowadzeniem do cyberprzestrzeni i jaki to może mieć wpływ na możliwość jej opracowania. Ważne jest identyfikowanie błędów (albo przynajmniej świadomość możliwości ich wystąpienia) na etapie wprowadzania danych i ich wpływu na kształt analizy, zwłaszcza wnioskowania.
3. *Błędy poznawcze* – wynikają z subiektywnych procesów myślowych związanych z przetwarzaniem informacji przez człowieka i stanowią konsekwencję redukowania rzeczywistości w celu jej szybszego zrozumienia. Błędy poznawcze mają związek z emocjonalnym stosunkiem analityka do jego pracy (produktów). Klasyczne błędy wynikają z myślenia życzeniowego albo syndromu myślenia grupowego bądź wartościowania analizowanej rzeczywistości ze względu na pozamerytoryczne parametry (w oparciu o arbitralnie przyjęte kryteria nieuwzględnione w procesie badawczym albo planie analizy). Każdy analityk musi sobie zdawać sprawę z błędów poznawczych, być świadomym istnienia schematów myślenia narażających analityka na porażkę – tak w zakresie myślenia kontekstowego, jak i krytycznego. Ważna jest relacja błędów poznawczych z pozostałymi zmiennymi składającymi się na całokształt

myślenia kontekstowego w domenie bezpieczeństwa. W tym zakresie sztuczna inteligencja ma wyraźną przewagę nad człowiekiem. Z drugiej strony jednak, algorytm musi uwzględniać, że analizowane dane mogą być obarczone błędami poznawczymi. W konsekwencji sztuczna inteligencja nie tylko powinna rozpoznawać okoliczności zwiększające prawdopodobieństwo wystąpienia błędów poznawczych na etapie zbierania i przetwarzania danych, ale także wiedzieć, w jaki sposób sobie z nimi radzić. Tutaj wydaje się, że konieczne jest jej trenowanie przez doświadczonych analityków. Chociażby w kontekście analizowania zjawisk społecznych/politycznych/militarnych przez reprezentantów określonych grup lintersu – narodowych, politycznych czy wojujących stron – roszczących sobie prawo do bycia obiektywnym.

4. *Procedury kodowania i dekodowania informacji z danych* – w myśleniu kontekstowym konieczna jest świadomość występowania relacji dane – informacje, czyli reprezentacji informacji i samej informacji. W systemach teleinformatycznych jest to dosyć oczywiste i cyberprzestrzeń opiera się na *świadomości* tej relacji, która jest na bieżąco wykorzystywana przez algorytmy. Problem może się pojawić kiedy przeniesiemy tę relację na analizowane zjawiska bezpieczeństwa, tj. relację pomiędzy wskaźnikiem a zmienną – o tym jednak już dalej, przy omawianiu myślenia krytycznego. Co do zasady jednak w kontekście procedury kodowania i dekodowania danych – wydaje się, że AI w tym obszarze jest w stanie optymalizować i przyspieszać proces analityczny. Zwłaszcza w zakresie pracy na dużych ilościach danych (por. D. Prokopowicz, A. Gołębiowska, M. Such-Pyrgiel, 2023).
5. *Wpływ czynników zewnętrznych na obniżenie wiarygodności informacji i analiz* – procedura analityczna jest narażona na wpływ czynników zewnętrznych związanych z presją psychiczną, oczekiwanymi rezultatami analizy, ulokowaniem analityka w strukturze organizacji, wpływem politycznym. Wpływ tak skatalogowanych czynników zewnętrznych na każdym etapie procesu analitycznego powinien być właśnie wychwycony przez sztuczną inteligencję.

Myślenie krytyczne w domenie bezpieczeństwa a potencjał sztucznej inteligencji

Z perspektywy analizy bezpieczeństwa kluczowe znaczenie ma *odnalezienie się* analityka na poszczególnych etapach cyklu wywiadowczego. Istotna jest również świadomość specyfiki samego cyklu. Przez cykl wywiadowczy należy rozumieć pięcioetapowy proces, na który składa się *(I) Planowanie i kierowanie, (II) Gromadzenie, (III) Przetwarzanie, (IV) Analiza, (V) Rozpowszechnianie/Dystrybucja* (CIA). Mówiąc o analizie wywiadowczej należy wskazać, że chodzi o konkretne procesy umysłowe, w oparciu o które ludzie budują własne modele, schematy – te z kolei służą do przetwarzania informacji (R. J. Heuer, 1999, s. ix). W tym kontekście pojawia się pytanie: ***Czy sztuczna inteligencja jest w stanie samodzielnie budować i modyfikować modele i schematy konieczne do przetwarzania i analizowania informacji?*** Wydaje się, że dokładnie do tego została wykreowana, jednak nie dzieje się to w oparciu o procesy umysłowe, ale samouczące się algorytmy, których potencjał jest jednak uzależniony od partnerów interakcji oraz ich architektury. Dotyczy to zarówno podmiotów wprowadzających dane do modeli uczenia maszynowego, jak i samego przebiegu tego procesu.

Z uwagi na powyższe, myślenie krytyczne – jako uzupełnienie myślenia kontekstowego, z którym się warunkuje i wzajemnie przenika – kreuje wyobraźnię analityczną. W konsekwencji myślenie krytyczne, przede wszystkim właściwe dla domeny bezpieczeństwa – ale nie tylko – polega na prowadzeniu analiz, których rezultaty to konkretne produkty analityczne, uwzględniających następujące zasady:

1. *Ograniczonego zaufania do własnych wiedzy/kompetencji/umiejęt*ności – analityk musi być świadomy zakresu swojej niewiedzy, braku ewentualnych kompetencji bądź umiejętności. Tylko wówczas będzie w stanie je uzupełnić, nadrobić bądź wzmocnić. To powoduje, że na każdym z etapów cyklu wywiadowczego konieczne jest ograniczone zaufanie do własnych kompetencji i otwarcie na konstruktywną krytykę. To wymaga dystansu do własnej pracy analitycznej i produktów, jakie się opracowuje. Wydaje się, że AI jeszcze nie ma własnej refleksji w przedmiotowym obszarze, pomimo że potrafi definiować zakresy własnej niewiedzy i dążyć do jej uzupełnienia.

2. *Rozróżnienia faktów od opinii* – to elementarna zasada związana z myśleniem krytycznym, która jest odzwierciedlona w podstawowym rozróżnieniu części składowych dokumentacji analitycznej wyodrębniającym a) stan faktyczny; b) opinie/oceny omówionego stanu faktycznego; c) wnioski; d) rekomendacje. Ważne jest aby taki materiał był sporządzony w sposób, który nie będzie przenosił treści pomiędzy wskazanymi częściami składowymi. Najbardziej niebezpieczne jest omawianie stanu faktycznego poprzez wykorzystanie do niego własnych ocen i opinii – ewentualnie zapożyczonych, ale przedstawianych jako własne. W tym kontekście należy zaznaczyć, że sztuczna inteligencja posiada przynajmniej bazowe umiejętności w przedmiotowym zakresie. Na podstawie uczenia się i rozwijanej sukcesywnie analizy językowej wydaje się, że taka kompetencja AI jest już częściowo dostępna.
3. *Kwestionowania rozwiązań oczywistych* – każdy człowiek dąży do uproszczenia procesu wnioskowania oraz stworzenia generalnych modeli myślenia o rzeczywistości (por. R. J. Heuer, 1999, s. ix). Taki mechanizm w dużym zakresie powinien ułatwić (przyśpieszyć oraz usprawnić) podejmowanie decyzji poprzedzonej sprawnym wnioskowaniem. W tym kontekście istotna jest jednak świadomość płynności i złożoności fenomenu bezpieczeństwa, który z uwagi na charakter środowiska (otoczenia społecznego) permanentnie się zmienia. Zwłaszcza w kontekście funkcjonowania grup interesu oraz dynamiki postrzegania bezpieczeństwa i rozpoznawania jego stanu faktycznego w oparciu o subiektywne odczucia aktorów społecznych. Tak przeprowadzone dekodowanie stanu bezpieczeństwa może doprowadzić do tego, że oczywiste rozwiązania, jakie intuicyjnie się nasuwają, są rezultatem błędów poznawczych i barku odpowiedniego przygotowania. Tutaj AI może mieć, przynajmniej na obecnym etapie, spore problemy z łamaniem własnych schematów, jakie zostały jej narzucone przez programistów, a później dopiero rozwijane w ramach komunikacji i interakcji w cyberprzestrzeni.
4. *Wystrzegania się redukcjonizmu* – w poszukiwaniu najprostszych oraz najbardziej oczywistych rozwiązań, czasem schematy myślenia przybierają postać redukcjonizmu. Świadomość niedoskonałości własnych

schematów prowadzonej pracy analitycznej i ograniczeń, jakie towarzyszą procesom zbierania informacji oraz syntezie – bezpośrednio nawiązuje do poprzedniej cechy, czyli kwestionowania rozwiązań oczywistych. Pomimo że jest to inna cecha myślenia krytycznego, to dążenie do uproszczenia procesów poznawczych powoduje, że przeszacowujemy albo nie doceniamy wpływu pewnych zmiennych na kształt zjawisk i środowiska bezpieczeństwa. Uwaga dotycząca możliwości sztucznej inteligencji związanych z wystrzeganiem się redukcjonizmu jest analogiczna zatem, jak przypadku kwestionowania rozwiązań oczywistych.

5. *Uwzględniania struktury interesów na każdym etapie pracy z informacją* – zmienna ta pośrednio odwołuje się do *charakterystyki źródeł informacji* przywołanej jako cecha/zmienna myślenia kontekstowego. Przy czym tylko częściowo należy rozumieć te obszary wyobraźni analitycznej jako nakładające się na siebie. Analityk bezpieczeństwa musi uwzględnić strukturę interesów w prowadzonej pracy zarówno w kontekście właściwości przetwarzanych informacji przez poszczególne podmioty (w tym aktorów społecznych) w cyberprzestrzeni, ale i samych podmiotów bezpieczeństwa, które następnie poddają te informacje subiektywnej (czasem skrajnie subiektywnej) ocenie.
6. *Wykorzystania wyobraźni do badania i weryfikowania hipotez* – zanim hipoteza zostanie zbadana i następnie zweryfikowana lub sfalsyfikowana, musi się w ogóle pojawić. Stawianie hipotez, oprócz definiowania problemu badawczego, celu badań oraz pytań szczegółowych – jest kwintesencją fazy konceptualizacyjnej procesu badawczego, ale także i analitycznego *per se*. W tej właśnie fazie kluczową rolę odgrywa wyobraźnia i jej funkcja kreacyjna. Z uwagi na powyższe, samo badanie hipotez nie będzie niczym niezwykłym dla AI, jednak pod warunkiem, że zostaną one w prawidłowy sposób postawione przez człowieka. Sztuczna inteligencja najprawdopodobniej będzie się wzorować podczas budowania własnych hipotez na takich, które znajdzie w cyberprzestrzeni. Będzie to miało najpewniej pewną formę naśladownictwa. Z drugiej strony należy przyjąć, że to tylko kwestia czasu, kiedy AI będzie sprawnie funkcjonować w fazie konceptualizacyjnej procesów analitycznych.

7. *Dekodowania zmiennych w oparciu i wskaźniki* – zmienne powinny być wyodrębnione z pytań badawczych, hipotez oraz innych zdarzeń i okoliczności związanych z rzeczywistością społeczną (systemem bezpieczeństwa), co musi uwzględniać ich specyfikę. Jednym z kryterium wyodrębniania zmiennych jest możliwość ich zmierzenia za pośrednictwem wskaźników. Dekodowanie zmiennych w oparciu o wskaźniki wymaga praktycznie wszystkich elementów składających się na myślenie kontekstowe oraz krytyczne. Stanowi kwintesencję wnioskowania, którego rolą jest eksplantacja procesów bezpieczeństwa. Wymaga połączenia funkcji kreacyjnej wyobraźni analitycznej z wiedzą praktyczną z domeny bezpieczeństwa. W tym zakresie sztuczna inteligencja ma jeszcze dużo do zrobienia, jednak jest tylko kwestą czasu, kiedy odpowiednie algorytmy nabiorą odpowiednich kompetencji (jeżeli już nie nabrały).

Zakończenie

W tekście omówiono łącznie dwanaście cech wyobraźni analitycznej wykorzystywanej w domenie bezpieczeństwa – odpowiednio pięć dotyczących myślenia kontekstowego oraz siedem związanych z myśleniem krytycznym. Łącznie na dwanaście cech/zmiennych, które składają się na wyobraźnię analityczną, już na chwilę obecną sztuczna inteligencja sprawnie funkcjonuje (albo zaraz będzie sprawnie funkcjonować) praktycznie we wszystkich. Naturalnie jedne są jej bliższe i łatwiej się AI w nich odnajduje (np. unikanie błędów poznawczych oraz wpływu czynników zewnętrznych na obniżenie wiarygodności informacji i analiz), z drugiej strony problematyczne jest, i pewnie przez pewien czas będzie, przestrzeganie zasady *Ograniczonego zaufania do własnych wiedzy/kompetencji/umiejętności.* Przede wszystkim takie podejście zakłada, że istnieje zaufanie analityka do samego siebie w związku z prowadzonymi analizami. Wydaje się, że sztuczna inteligencja wartościuje, analizuje i koryguje własną metodykę pracy, pod kątem jej przydatności do realizacji postawionego zadania.

Kolejnym etapem w badaniach możliwości wykorzystania sztucznej inteligencji w analizie bezpieczeństwa, jest uchwycenie i omówienie procesów powstawania świadomości (bądź jej funkcjonalnego odpowiednika) jakimi cechuje się sztuczna inteligencja oraz człowiek.

Bibliografia

Chałubińska-Jentkiewicz, K. (2019). *Cyberbezpieczeństwo – zagadnienia definicyjne*, Cybersecurity and Law 2019; 2(2).

Chrost, M. (2021). *Refleksyjna samoświadomość i działanie osoby,* Paedagogia Christiana 1/47.

Ciesielski, M. (2019). *Socjologia bezpieczeństwa jako subdyscyplina nauk o bezpieczeństwie*, Cybersecurity and Law Nr 2(2).

Ciesielski, M. (2024). *Dyskurs o bezpieczeństwie a media*, Cybersecurity and Law Nr 2 (12).

Cukier, K., Mayer-Schönberger, V., de Véricourt, F. (2022). *Myślenie kontekstowe. Największa przewaga ludzi nad sztuczną inteligencją,* MT Biznaes, Warszawa .

Heuer, R. J. (2024). *Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Central Intelligence Agency 1999. Pozycja dostępna na stronie Centralnej Agencji Wywiadowczej chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cia.gov/resources/csi/static/Pyschology-of-Intelligence-Analysis.pdf [dostęp: 11.12.2024 r.)

Kubera, G. (2024). *Mało kto wie, czym zajmuje się firma miliardera. Wśród klientów są CIA i FBI,* https://businessinsider.com.pl/technologie/tajemniczy-biznes-miliardera-palantir-obsluguje-cia-i-fbi/m417c6j [dostęp: 9.12.2024 r.].

www.palantir.com/ [dostęp: 9.12.2024 r.).

Prokopowicz, D., Gołębiowska, A., Such-Pyrgiel, M. (2023). *The role of Big Data and Data Science in the context of information security and cybersecurity,* Journal of Modern Science, 53(4):9-42.

Wright Mills, C. (2008). *Wyobraźnia socjologiczna,* Wydawnictwo Naukowe PWN, Warszawa.

Strony internetowe

CIA – chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cia.gov/spy-kids/static/59d238b4b5f69e0497325e49f0769acf/Briefing-intelligence-cycle.pdf