UNIWERSYTET Andrzeja Frycza Modrzewskiego w Krakowie

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE

e-ISSN 2451-0718
ISSN 1899-6264

2026
Nr 2

Copyright© 2026 by the Author(s)
This is an open access article under the CC BY-NC-ND 4.0 license

https://doi.org/10.31749/2451-0718-btip-2026-2-005
Received: 15.05.2026
Accepted: 9.09.2026

Selected Aspects of Intelligence Services' Recruitment of Sources in Online Environments: Characteristics, Threats and Countermeasures

Janusz Liber

Lt Col (Retd), PhD, Eng, Faculty of Security Sciences, Andrzej Frycz Modrzewski Krakow University, Kraków, Poland
https://orcid.org/0000-0003-4562-4661

Introduction

The threat of cyber warfare is causing growing concern across intelligence communities worldwide. "In June 2009, the United States Cyber Command was established, and in July 2011, Deputy Secretary of Defense William J. Lynn III announced that, as a matter of doctrine, cyberspace would be treated as an operational domain similar to land, air, sea, and space" (Colarik, Janczewski, 2012: 35). Cyber warfare is conducted through the infiltration of computer networks in order to cause damage and/or disruption to various forms of infrastructure. It may also encompass intelligence collection and sabotage operations directed against specific targets, such as military installations and power grids. The threat of cyber warfare affects every state in the international system (Maloney, 2019). Cyber intelligence fosters the development of tools designed to compromise computer networks and standalone systems. Such activities are undertaken by government organizations, national intelligence agencies, armed forces and private commercial entities that openly develop cyber-attack technologies (Andress, Winterfeld, 2011).

Due to the migration of certain intelligence activities into cyberspace, intelligence specialists and available information concerning contemporary online intelligence operations indicate that human sources of information – the fundamental component of human intelligence (HUMINT) – continue to be regarded as highly credible and valuable (Lowenthal, 2012: 520). Consequently, agent recruitment is increasingly conducted within the virtual environment (Cheatham, 2019).

Human intelligence is a category of intelligence activity in which information is obtained from human sources (AAP-6, 2013: 233). Agent recruitment is carried out by specialized intelligence units. Unlike other intelligence collection methods, HUMINT operations conducted in the physical world involve increased security risks for the individuals directly engaged in such activities.

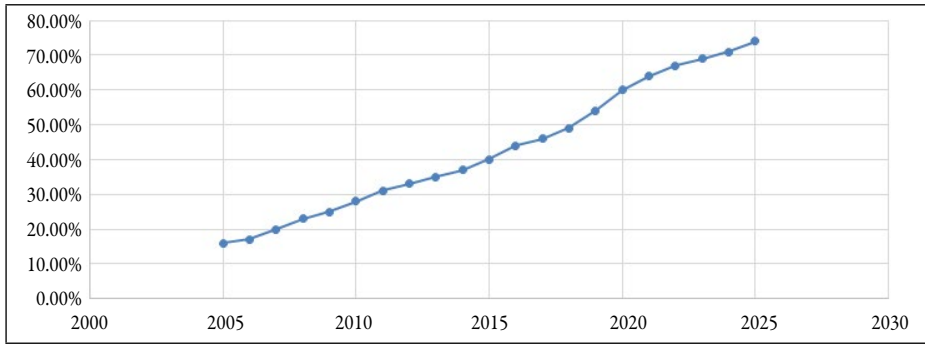
In traditional HUMINT operations, a prerequisite for conducting intelligence activities is often the deployment of intelligence personnel abroad in order to identify, recruit and handle human sources of information. Case officers frequently operate in environments where their very presence may jeopardize the success of ongoing operations. Furthermore, intelligence targets are often individuals subject to counter-intelligence protection; therefore, even physical contact with them may constitute a high-risk activity.

HUMINT activities are typically conducted by two groups of officers. The first operates under diplomatic cover and benefits from diplomatic immunity, which may reduce some of the risks associated with intelligence work. The second consists of military personnel and HUMINT officers operating without immunity, often posing as businesspeople, tourists or specialists in various fields while utilizing false identities. These risks are further compounded by the limited number of agents and case officers who can physically travel to and from areas of intelligence interest. It should also be noted that many areas of significant intelligence interest are highly protected and exceptionally difficult for outsiders to access, regardless of their ability to assimilate safely into the target environment (Howard, 2007).

Current trends in human intelligence focus increasingly on the identification, recruitment and handling of human sources within the virtual environment. This approach not only reflects contemporary developments in intelligence practice, as discussed below, but also serves as a means of reducing the risks outlined above. Online recruitment and agent handling can effectively complement traditional HUMINT methods, enhancing both operational security and the safety of those involved.

The developments in intelligence activities described above are, among other factors, a response to the rapid expansion of the internet and the continuing migration of individuals from the physical to the virtual world. Over the past two decades, the online environment has expanded dramatically. By 2025, approximately 74 per cent of the world's population – around six billion people – were using the internet. Figure 1 illustrates the proportion of the global population using the internet between 2005 and 2025.

Figure 1. Global internet user penetration (% of population), 2005–2025



Source: *Individuals using the Internet* (2025).

Users are increasingly turning to the internet to foster social connections, play games, establish intimate relationships and seek employment. Globally, nearly two-thirds of the population uses social media, amounting to approximately 5.4 billion users, or roughly 65% of the world's population. Daily active users spend an average of two hours and 21 minutes on social media platforms. Furthermore, the average individual uses 6.8 different social networks each month, reflecting the vast ecosystem of available digital platforms. On a weekly basis, 65 million people use LinkedIn to search for employment opportunities, and 28 million have added the #OpenToWork frame to their profiles. Consequently, six people are hired through LinkedIn every minute (Onyango, 2026).

These developments have triggered profound transformations across numerous sectors, ranging from sales, marketing, education, and management to intelligence operations. As a result, the processes of spotting prospective candidates and recruiting agents – the core components of human intelligence (HUMINT) – are now conducted both in traditional physical environments and within cyberspace (Department of Defence, 2013).

HUMINT operations provide decision-makers with critical information required for strategic decision-making in the political, military and economic spheres. Criminal enterprises and terrorist organizations typically operate as closed environments, making them highly resilient to technical surveillance and undercover operations alone (Murphy, 2007: 7, 10). This operational constraint is particularly acute in hard-to-penetrate regions characterized by weak state institutions, limited diplomatic access or deeply insulated communities (Johnson, 2010: 308–332).

Similar intelligence collection challenges exist in states protected by sophisticated and comprehensive intelligence and counterintelligence programmes managed by professional security services (Rotberg, 2003: 3). Overcoming these barriers often depends on recruiting an informant with direct access to the required information or developing agents capable of obtaining such access. By leveraging

a human source embedded within a target organization, governments can more effectively identify, understand and assess an adversary's intentions, capabilities and vulnerabilities (Shepherd, 2009).

This article aims to elucidate the specific nature of cyber-recruitment operations conducted by intelligence agencies while exploring ways to strengthen the resilience of individuals, societies and state institutions against such hostile activities. The primary research question is formulated as follows: How do intelligence services conduct online agent recruitment, and what countermeasures should be implemented to enhance stakeholder resilience against such operations? In order to address the research problems posed, the author employed the following research techniques: a systematic literature review, a critical literature review and a case study. Because the concept of cyber HUMINT is relatively novel, the subject literature contains a limited number of studies within this specific scope. The literature that underwent analysis was divided into three principal categories: materials concerning "classical" HUMINT, studies dedicated to online human intelligence activities, including publications on relationship-building in virtual environments, and classified government materials disclosed by whistleblowers.

The Recruitment of Human Intelligence Sources

"Traditional" intelligence operations are characterized as "activities or actions [...] designed to influence political, economic, or military conditions abroad, where the role of the [...] government will not be apparent or acknowledged publicly" (Lowenthal, 2012). The British intelligence agency GCHQ uses a similar term to describe offensive operations in cyberspace, referring to them as "cyber effects operations". These operations are based on the premise that, although conducted in a virtual environment, they "produce real-world effects" (Snowden, 2014). For the purposes of this article, the author defines Cyber-HUMINT as "standard" human intelligence operations conducted within cyberspace by specialized intelligence service units.

Human intelligence (HUMINT) activities generally follow a standard cycle for the development and management of human sources of information. Typically, the recruitment and agent-handling cycle consists of six stages (Burkett, 2013: 13):

- identification of an individual capable of providing the required information;
- assessment of the identified individual in terms of their access to critical information, motivations for cooperation and vulnerability to recruitment;
- development of a relationship with the prospective source in order to further assess their access, motivation, vulnerability and suitability;
- recruitment;
- source handling, including training, tasking and performance evaluation;
- transfer of the agent to another case officer or termination of cooperation.

In pursuing these objectives, HUMINT officers employ a variety of methods and techniques designed to successfully complete the recruitment process, as described in both intelligence theory and psychological research, which are discussed later in this article.

The Cyber-HUMINT methodology, which emerged around 2010, demonstrates that cooperation between human intelligence specialists and cyber security experts, combined with the application of social engineering techniques, constitutes one of the principal strengths of this intelligence discipline. This approach introduced an innovative information security model that integrates traditional HUMINT concepts with social engineering techniques, including the use of avatars by intelligence officers operating in cyberspace and the dissemination of information and disinformation within virtual environments (Steinhart, 2014). This form of intelligence activity emerged through the combination of the technical expertise of cyber security specialists and the operational experience of HUMINT practitioners (Condliffe, 2014).

The operations in question involve intelligence officers establishing contact with a specific individual and developing a relationship in a manner similar to that employed by traditional HUMINT officers; however, part of this process is conducted in cyberspace. To this end, intelligence services may utilize online discussion forums, social media platforms, online games (Dori, 2015) and other internet-based services (Carruthers, 2018). Such activities may form part of a broader intelligence operation in which intelligence services create, operate and monitor online forums, honeypots, and other digital platforms designed to identify, assess and engage potential targets.

As indicated above, the key elements of agent recruitment involve identifying and assessing candidates' vulnerabilities and motivations, a process that is facilitated through establishing and developing relationships with targeted individuals. Social media platforms play a significant role in this regard, as they enable the profiling of prospective recruits. For example, LinkedIn provides information about users' educational backgrounds and professional experience, allowing recruiters to offer employment or consultancy opportunities without arousing suspicion. Facebook, in turn, offers insights into users' interests, personal preferences and social networks.

One of the technical aspects of Cyber-HUMINT that is particularly useful in agent recruitment is the ability to extract large volumes of data from social media platforms. A notable example is LinkedIn data scraping, which can be conducted using automated tools designed to collect information from user profiles, including job titles and email addresses, and export it into formats such as CSV files or Google Sheets. These tools often employ browser extensions or cloud-based bots to circumvent platform restrictions. According to industry sources, a commonly recommended limit for avoiding detection is approximately 1,500 profile extractions per day ("15 LinkedIn Scraper Tools", 2026).

The developments described above have prompted a reassessment of agent recruitment methods. During the Cold War and the period immediately following it,

individuals who agreed to cooperate with intelligence services were most often motivated by factors encapsulated in the MICE model: Money, Ideology, Coercion (or Compromise) and Ego. Contemporary intelligence analyses suggest that the explanatory value of this model has diminished, as case officers increasingly seek to recruit non-state actors whose motivations are shaped by complex and often competing loyalties relating to family, religion, ethnicity, nationality and other social affiliations. In light of these developments, it has been argued that HUMINT practices should incorporate insights from social psychology, particularly the principles of reciprocity, scarcity, authority, commitment and consistency, liking, and consensus, as additional tools for understanding and influencing human behaviour (Burkett, 2013).

This postulate is illustrated by a PRC intelligence operation in which Ho, an assistant to the Secretary-General of Taiwan's National Security Council, was recruited. In analyzing the circumstances of this recruitment, it has been proposed that the MICE model be expanded to MICE-R. In the case under discussion, the "M" component played a role, as the agent who was recruited received financial remuneration from the intelligence services; however, given that the recruitment was conducted through a long-standing mutual acquaintance, it has been suggested that an additional "R" component – referring to *renqing*, meaning rapport and reciprocity grounded in personal relationships – should be added to the MICE model. It was precisely *renqing* that Huang exploited when recruiting Ho through a mutual friend ("Pamir Special Commentary", 2025).

Although there is no consensus on this issue, a body of literature and available data supports the thesis that virtual relationships involve strong emotional bonds. A key question is whether such online bonds are as strong as those developed in offline environments. For many researchers, the answer is affirmative. For instance, Facebook has proven to be an effective tool for building social connections, enabling users to develop relationships similar to those formed offline (Grieve et al., 2013: 608). There are also studies suggesting that virtual bonds may be even stronger than those developed in offline contexts. This claim is based on the notion that online interactions can reduce social inhibitions and lead to greater openness (Ratan et al., 2010). One study on MMO games demonstrated that disinhibition led players to disclose more personal information, resulting in higher levels of trust (Cole, Griffiths, 2007). Evidence from practice appears to support these findings, as members of the "War Thunder" community have repeatedly disclosed classified military documents on the forum (Czajkowski, 2024).

JTRIG materials indicate that, during online intelligence operations, principles of social psychology applied in marketing and advertising were considered particularly useful. The literature on the subject further highlights knowledge of foreign languages and cultural factors, as well as identity management and the dynamics of relationship-building, as key elements influencing the creation and maintenance of online contacts (Dhami, 2015).

Case Study

At the beginning of 2017, a GE Aviation engineer received a message via LinkedIn. The message originated from a man claiming to be an employee of the Nanjing University of Aeronautics and Astronautics. In March, the two individuals began exchanging emails. The engineer was subsequently invited to Nanjing for an academic "exchange" based on his experience at GE Aviation. He agreed to deliver a presentation entitled "Analysis of composite structure design for the aerospace industry and manufacturing technology development". On 25 May 2017, the engineer transferred five GE Aviation documents to a private laptop and travelled to China. While delivering the presentation, he encountered technical difficulties and therefore permitted the university employee to connect a USB drive to the laptop containing all five documents. It reportedly took only a few months for the intelligence service to persuade the engineer to accept the offer: a fee of $3,500 for a one-hour presentation, along with coverage of travel, accommodation and catering expenses (Cheatham, 2019).

In 2019, India identified 150 social media profiles allegedly used by Pakistan to target Indian Army officers and extract state secrets. The issue was considered sufficiently serious that India ordered soldiers to remove Facebook, Instagram, Tinder and numerous other applications from their mobile devices. The process typically began with a female profile "liking" a soldier's post on social media and requesting additional photographs of military equipment. Subsequently, the interaction would develop into direct messaging, during which individuals purportedly linked to Pakistani military intelligence would attempt to elicit sensitive information ("Pakistan Using Honeytrap", 2019).

In 2026, the NATO community was shaken by the case of a Greek Air Force officer allegedly recruited by Chinese intelligence services. Available information suggests that Colonel Christos Flessas, who served in the 128 Telecommunications and Electronics Training Group, maintained a LinkedIn account on which he had published a detailed CV. Contact with the individual in question was initiated via the platform, where unidentified persons, acting on behalf of a Malaysia-based company providing consultancy services to Asian countries, offered the officer a collaboration.

Initially, Flessas conducted research for a website; however, the situation gradually escalated during a trip to Beijing, where he met three directors of the company for which he was carrying out tasks. Greek authorities hypothesized that, under this cover, the officer may have been approached by representatives of Chinese intelligence services seeking to assess his knowledge and reliability. Subsequently, Flessas began receiving requests to share increasingly sensitive materials. The officer stated that as the volume of information he provided increased, so did his financial remuneration.

An individual known as "Steven" also emerged, acting as the intermediary responsible for communication with Flessas and the transfer of funds. "Steven" deposited amounts of up to €5,000 per month or €15,000 quarterly into the officer's

cryptocurrency wallet. To avoid detection, the officer made small withdrawals of €200–300 from ATMs. The transactions were carried out using a debit card issued in Hong Kong in the name of a third party. Using this card, funds could be withdrawn from any ATM worldwide.

The officer confessed to photographing and transmitting classified NATO documents using specialized encryption software allegedly provided by Chinese intelligence. The investigation indicated that the officer's consent to recruitment – most likely following intelligence-related engagement during his trip to China – was driven by financial gain and a desire for professional recognition ("Wake-up call", 2026; "Προφυλακιστέος ο σμήναρχος", 2026).

Conclusions

Given the specific nature of human intelligence operations described in this article, it should be noted that the shifting of certain intelligence activities into cyberspace represents a response to the migration of much of society into the virtual environment. Cyber-HUMINT operations enable access to targets that are otherwise difficult to reach or entirely inaccessible to traditional human intelligence, while simultaneously enhancing the safety of officers involved in the recruitment and handling of agents.

The enhancement of HUMINT operational parameters implies an increase in the number of potential human intelligence targets, as well as their vulnerability to recruitment. These circumstances necessitate the transfer of certain counter-intelligence activities into cyberspace, along with the adaptation of counter-intelligence preventive measures to emerging risks.

The primary vulnerabilities of Cyber-HUMINT operations lie in the conditions under which agents are recruited and handled online. Such activities are often conducted anonymously within gaming environments, discussion forums and social media platforms, where users naturally exchange information, share interests, establish contacts or seek employment. These interactions most frequently occur during leisure time, outside the workplace, which complicates or prevents the application of conventional cybersecurity measures. Understanding these psychological and social dynamics is therefore essential for those tasked with identifying and mitigating such threats.

Cyber-HUMINT operations draw upon principles of social psychology, including those applied in marketing and advertising, as well as elements of social engineering. Emotional manipulation – within MMO environments, the offering of consultancy services, requests for assistance with academic research, or the pursuit of "no-strings-attached" relationships – serve as examples of relationship-building strategies employed by human intelligence specialists in cyberspace. Given that

these behaviours are natural for internet users, only appropriately trained individuals are able to identify them as potential intelligence-related threats.

Online recruitment thus represents a sophisticated multifaceted intelligence methodology whereby operatives identify and recruit targets through virtual channels, exploiting psychological vulnerabilities and social engineering techniques. Effective counter-measures demand an integrated approach combining individual awareness, protective procedures and regular security training. Target resilience is substantially enhanced through psychological stability, threat awareness, rigorous organizational security protocols, and institutional cultures that facilitate the reporting of suspicious contacts. Such measures must address the evolving threat landscape of contemporary online recruitment operations.

In conclusion, it should be emphasized that the primary task of counter-intelligence protection, as part of building resilience against recruitment by intelligence services in cyberspace, is the detection and mitigation of factors conducive to such operations. Counter-intelligence services should train individuals, groups and institutions that may constitute potential targets of hostile intelligence services to recognize these threats and encourage them to report identified risk indicators.

This comprehensive training must be structured to address multiple dimensions of stakeholder attitudes in order to achieve sustainable counter-intelligence resilience. The intervention, implemented as part of counter-intelligence preventive measures, should take three dimensions of shaping stakeholder attitudes into account: the cognitive dimension, encompassing knowledge of threats and methods of response, the emotional dimension, aimed at fostering positive attitudes towards preventive initiatives, and the behavioural dimension, focused on shaping habits and responses to specific threats emerging in cyberspace.

References

AAP-6. Słownik terminów i definicji NATO. Biuro Standaryzacji NATO. https://wcnjik.wp.mil.pl/u/AAP6PL.pdf [accessed: 27.04.2026].

Andress, J., Winterfeld, S. (2011). *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners*. Syngress.

Burkett, R. (2013). An Alternative Framework for Agent Recruitment: From MICE to RASCLS. *Studies in Intelligence*, *57*(1), 7–17. https://calhoun.nps.edu/server/api/core/bitstreams/a2cb7f23-10f2-464b-9eae-30d9c5a476fa/content [accessed: 10.04.2026].

Carruthers, W.R. (2018). *Covert Action and Cyber Offensive Operations: Revisiting Traditional Approaches in Light of New Technology*. University of Salford, School of Arts and Media.

Cheatham, C. (2019). *I-Team: How the Cincinnati FBI cracked the Chinese spy case at GE Aviation*, Scripps Media, 4.03. https://www.wcpo.com/news/local-news/i-team/i-team-how-the-cincinnati-fbi-cracked-the-chinese-spy-case-at-ge-aviation [accessed: 10.04.2026].

Colarik, A., Janczewski, L. (2012). Establishing Cyber Warfare Doctrine. *Journal of Strategic Security*, *5*(1), 31–48. https://www.jstor.org/stable/26463986?seq=9 [accessed: 10.04.2026].

Cole, H., Griffiths, M.D. (2007). Social Interactions in Massively Multiplayer Online Role-Playing Gamers. *Cyberpsychology, Behavior, and Social Networking*, *10*(4), 575–583. https://doi.org/10.1089/cpb.2007.9988

Condliffe, J. (2014). *UK Intelligence Has Endorsed Cyber Security Courses For Wannabe Spies*, Gizmodo, 4.08. https://gizmodo.com/uk-intelligence-has-endorsed-cyber-security-courses-for-1615638319 [accessed: 27.03.2026].

Czajkowski, P. (2024). *Tajne dokumenty wojskowe znów wyciekły na forum War Thunder*, Ithardware, 23.12. https://ithardware.pl/aktualnosci/war_thunder_tajne_dokumenty_wojskowe-37538.html [accessed: 13.05.2026].

Department of Defense (2013). Department of Defense Instruction S-3325.10, Subject: Human Intelligence (HUMINT) Activities in Cyberspace, June 6, 2013. Secret/Noforn. https://nsarchive.gwu.edu/document/21378-document-19 [accessed 14.05.2026].

Dhami, M.K. (2015). *Behavioural Science Support for JTRIG's (Joint Threat Research and Intelligence Group's) Effects and Online HUMINT Operations*. https://www.statewatch.org/media/documents/news/2015/jun/behavioural-science-support-for-jtrigs-effects.pdf [accessed: 20.06.2022].

Dori, K. (2015). *Virtual HUMINT: conducting human intelligence operations in the virtual environment*, California. Naval Postgraduate School.

*15 LinkedIn Scraper Tools That Don't S*ck* (2026). Scrapp, 21.04. https://skrapp.io/blog/linkedin-scraper [accessed: 14.04.2026].

Grieve, R, Indian, M., Witteveen, K.G., Tolan, A., Marrington, J. (2013). Face-to-Face or Facebook: Can Social Connectedness Be Derived Online? *Computers in Human Behavior*, *29*(3), 604–609. https://doi.org/10.1016/j.chb.2012.11.017

Howard, R.D. (2007). *Intelligence in Denied Areas: New Concepts for a Changing Security Environment*, Joint Special Operations University. https://apps.dtic.mil/sti/tr/pdf/ADA495385.pdf [accessed: 14.05.2026].

Individuals using the Internet. (2025), ITU Statisctics, https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx [access: 14.05.2026].

Johnson, L.K. (2010). Evaluating "Humint": The Role of Foreign Agents in U.S. Security. *Comparative Strategy*, *29*(4), 308–332. https://doi.org/10.1080/01495933.2010.509635

Lowenthal, M.M. (2012). *Intelligence: From Secrets to Policy*, 5th Ed., CQ Press.

Maloney, L. (2019). *Cyber Warfare: Competing National Perspectives*, Modern Diplomacy, 11.03. https://moderndiplomacy.eu/2019/03/11/cyber-warfare-competing-national-perspectives [accessed: 14.05.2026].

Murphy, W.M. (2007). Oral Testimony. In *Law Enforcement Confidential Informant Practices* (pp. 7–10). U.S. Government Publishing Office.

Onyango, F. (2026). *Social Media Statistics – Users & Revenue*, Tridens Technology, 22.01. https://tridenstechnology.com/social-media-statistics/ [accessed: 12.10.2026].

Pakistan Using Honeytrap To Target Indian Army Officers, Says Minister (2019), NDTV, 9.12. https://www.ndtv.com/india-news/pakistan-using-honeytrap-to-target-indian-army-officers-says-minister-shripad-naik-2145995 [accessed: 14.05.2026].

Pamir Special Commentary: MICE-R? How Chinese intelligence services use "renqing" to collect intelligence in Taiwan (2025), Pamir, 23.04. https://pamirllc.com/blog/pamir-special-commentary-mice-r-how-chinese-intelligence-services-use-renqing-to-collect-intelligence-in-taiwan [accessed: 28.04.2026].

Προφυλακιστέος ο σμήναρχος που κατηγορείται για κατασκοπεία υπέρ της Κίνας: Οδηγήθηκε στις φυλακές Κορίνθου [Air Force Colonel accused of spying for China remanded in custody: Taken

to Corinth prison] (2026). Pronews, 10.02. https://www.pronews.gr/amyna-asfaleia/esoteriki-asfaleia/profylakisteos-o-54xronos-sminarxos-tis-polemikis-aeroporias-pou-katigoreitai-gia-kataskopeia-yper-tis-kinas [accessed: 14.04.2026].

Ratan, R.A., Chung, J.E., Shen, C., Williams, D., Marshall, S.P. (2010). Schmoozing and Smiting: Trust, Social Institutions, and Communication Patterns in an MMOG. *Journal of Computer-Mediated Communication*, *16*(1), 93–114. https://doi.org/10.1111/j.1083-6101.2010.01534.x

Rotberg, R.I. (2003). Failed States, Collapsed States, Weak States: Causes and Indicators. In R.I. Rotberg (Ed.). *State Failures and State Weakness in a Time of Terror* (pp. 1–25). The World Peace Foundation & The Brookings Institution Press.

Shepherd, R. (2009). *The Applications of Human Intelligence in Counterterrorism*, University of Calgary. http://dspace.ucalgary.ca/jspui/bitstream/1880/48904/1/2009_Shep-herd_MSS.pdf [accessed: 27.03.2026].

Snowden, E. (2014). *Exclusive: Snowden Docs Show British Spies Used Sex and 'Dirty Tricks'.* NBC News, 7.02. https://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-british-spies-used-sex-dirty-tricks-n23091 [accessed: 27.03.2026].

Steinhart, A. (2014). *The future is behind us? The human factor in cyber intelligence: Interplay between Cyber-HUMINT, Hackers and Social Engineering*, Diplomacy Journal, 31.03. https://web.archive.org/web/20140903143855/http://diplomacy.bg/archives/1190 [accessed: 28.04.2026].

'Wake-up call' for Greece as air force officer accused of spying for China. (2026). The Guardian, 10.02. https://www.theguardian.com/world/2026/feb/10/greek-air-force-officer-arrested-on-suspicion-of-spying-for-china [accessed: 12.05.2026].

Selected Aspects of Intelligence Services' Recruitment of Sources in Online Environments: Characteristics, Threats and Countermeasures

Abstract

This article examines the distinctive characteristics of agent recruitment within human intelligence (HUMINT) operations conducted in cyberspace. It analyzes selected modalities of informant recruitment employed by specialized HUMINT units operating in virtual environments, while simultaneously addressing the attendant risks and threats. Furthermore, it argues that the progressive migration of societal activity from the physical domain to the virtual sphere has significantly enhanced the strategic relevance of cyber-enabled human intelligence. The study posits that the principal mechanism for mitigating online recruitment efforts lies in the systematic enhancement of awareness among individuals who constitute potential intelligence targets, with regard to the methods, strategies and tradecraft employed by intelligence services. Ultimately, the article addresses a substantive gap in the existing literature concerning the recruitment of online information sources, conceptualizing this phenomenon as a strategic HUMINT response to the global population's transition into cyberspace.

Keywords: intelligence sources, agent recruitment, Cyber-HUMINT, cyberspace, social engineering

Author Contributions
Janusz Liber: Conceptualization, Methodology, Formal analysis, Investigation, Resources, Visualization, Writing – original draft, Writing – review & editing.

Supplementary Materials
Not applicable.

Funding
This research received no external funding.

Ethics Approval Statement
Not applicable.

Informed Consent Statement
Not applicable.

Data Availability Statement
Data sharing is not applicable to this article as no new data were generated or analyzed in this study.

Declaration of Generative AI Use
No artificial intelligence tools were used in the preparation of this manuscript.

Acknowledgments
Not applicable.

Conflict of Interest
Janusz Liber declares no conflict of interest.