УДК 327.7
DOI: 10.18384/2310-676X-2018-1-45-53

ЦИФРОВАЯ ЗАВИСИМОСТЬ НАТО

Курылев К.П., Цаканян В.Т.
Российский Университет Дружбы Народов
117198, г. Москва, ул. Миклухо-Маклая 10/2, Российская Федерация

Аннотация. В статье основное: освещена новейшая история кибербезопасности НАТО с учетом растущей роли киберпространства в стратегии, политике и трансформации вооруженных сил Альянса, а также других структур. В целом влияние киберпространства на системы военной обороны хорошо документировано во многих источниках, особенно на примере НАТО, что способствовало более полному изучению проблематики. НАТО была создана как организация, целью которой было обеспечение коллективной безопасности, кризисное управление и сотрудничество по безопасности в разных областях для государств-членов. Новые глобальные проблемы дали начало новым основным функциям безопасности организации. В ходе исследования были выявлены изменения, которые были спровоцированы влиянием цифрового пространства.

Ключевые слова: НАТО, коллективная безопасность, кибербезопасность, киберугрозы, «цифровое пространство».

DIGITAL DEPENDENCE OF NATO

K. Kurylev, V. Tsakanyan
Peoples' Friendship University of Russia
Miklikho-Maklaya str. 10/2, 117198, Moscow, Russian Federation

Abstract. This article focuses on the recent history of NATO's cyber defense and the increasing role of cyberspace on NATO's strategy, policy, and transformation of military forces, as well as the other elements of power. In general, the impact of cyberspace on the military defense systems is well documented in many sources, especially in the example of NATO. Due to this fact this problem was studied more profoundly. NATO was founded as an organization, the purpose of which was to ensure the collective defense, crisis management, and cooperative security in various spheres for its member nations. New global challenges gave a new birth to the core security functions of the organization. The study has resulted in showing the changes which cyberspace provoked.

Key words: NATO, collective defense, cyber defense, cyber threats, cyberspace.

Исторические процессы трансформировали европейское сообщество совместно с Канадой и Соединенными Штатами Америки в североатлантическое. Вся североатлантическая цивилизация столкнулась со своими представлениями об общих угрозах, что проявилась в необходимости ее защиты. Для противосто-

яния вызовам был создан союз стран НАТО. Организация Североатлантического Договора была основана в 1949 г. как оборонный альянс.

Процесс внутренней гармонизации командных структур, коммуникаций и военной промышленности привел к созданию самой мощной и успешной системы обороны в наши дни. Способность НАТО работать под одной командой подчеркивает не только ее военную силу, но и согласованные действия, которые устраняют многие недостатки в системе обороны. Будучи организацией коллективной обороны, НАТО должна противостоять любым угрозам, включая новые глобальные вызовы, как киберугрозы.

Впервые НАТО пострадало от значительных кибератак в 1999 г., во время операции ALLIED FORCE против Сербии, со стороны «патриотических хакеров» [7, с. 2]. Поскольку эти нападения были относительно незначительными, они были в основном проблемой для «мандата по борьбе с киберпреступностью» NCS, а не для «коллективной защиты», как бы ни интерпретировались в то время. Даже превышающие по масштабам кибератаки против Эстонии в 2007 г. не вызвали ответ по статье 5 Договора.

НАТО ясно указала в «Политике по Кибероборону» [6], что коллективная оборона действительно применяется в киберпространстве и даже обсуждала процесс, который Альянс будет использовать, чтобы ссылаться на коллективную оборону, – сохраняя двусмысленность в отношении конкретных пороговых значений. Этот процесс эскалации начинается с тактического (технического) уровня. Если инцидент имеет политические последствия для коллективной обороны, он будет рассматриваться через соответствующие технические и политические инстанции в Североатлантическом совете [7, с. 5]. Процесс консультаций по статье 4 в случае серьезной кибер-атаки также был рассмотрен [6]. Для создания единой и мощной структуры защиты членов организации по двум направлениям – «умная защита» и усиление «объединения и совместного использования», НАТО предусмотрела возможность развертывания групп быстрого реагирования NCIRC (RRT) [11].

Еще один шаг – создание Агентства связи и информации НАТО (NCI) [12], в результате слияния NATO Consultation, Command and Control Agency (NCIA), NATO ACCS Management Agency (NACMA) Программы ALTMB и Штаб-квартиры НАТО. Агентство NCI было создано для поддержки НАТО в ИТ сфере и C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). В ходе обсуждений в течение нескольких лет был создан проект под названием «Красная киберкоманда», предназначенный для проведения тестирования кибератак на системы НАТО, но также он может быть теоретически использован для поддержки членов Альянса и стран-партнеров. Учитывая появление общих угроз, соответственно и выявлялись новые подходы по их устранению, в итоге, просматривается эволюция системы безопасности НАТО.

Лидером в продвижении идеи по наращиванию кибернетических возможностей Альянса являлись Соединенные Штаты Америки. Белый дом заявил, что будет действовать по принципу ‘Casus foederis’ (“Договор-

ный случай") также и в виртуальном пространстве, утверждая, что: «Все государства обладают неотъемлемым правом на самооборону, и мы признаем, что некоторые враждебные действия, проводимые через киберпространство, могут натолкнуть нас на действия в рамках обязательств, которые мы имеем с нашими партнерами по военным договорам» [8, с. 14].

Исполняющий обязанности помощника министра обороны по вопросам обороны и глобальной безопасности Томас Аткин заявил в Комитете Палаты представителей США по вооружённым силам: «Мы все еще работаем над определением» того, в каком смысле «кибератака – акт войны». Белый дом и Пентагон дали понять, что в 2011 г. такие действия, как закрытие энергосистемы США посредством кибератаки, не всегда могут быть решены киберответами, а, возможно, «пусками ракет на один из ваших дымоходов», (добавил официальный представитель Министерства обороны США [9]). Тем не менее не все государства-члены разделяют ту же точку зрения, учитывая специфику информационного пространства.

Внешнеполитическая координация по кибербезопасности является одной из важнейших факторов по разработке формулировок киберугроз (табл.), что в дальнейшем ускорит выявление угроз и их своевременное устранение. Кибербезопасность как важный вопрос была отмечена в 2002 г. на саммите НАТО в Североатлантическом совете в Праге. Киберзащита как часть системы обороны становится достойной коллективных дискуссий Альянса [15]. Было решено создать техническую программу по кибербезопасности НАТО, которая будет основана на базе центра Способностей реагирования на компьютерные инциденты НАТО (NCIRC) [3].

Таблица

Содержание стратегического уровня встреч на высшем уровне НАТО, где кибербезопасность упоминается как важная область обороны

Встречи на высшем уровне Североатлантического совета НАТО	**Вопросы, связанные с кибербезопасностью в декларациях на высшем уровне**
Рига, Латвия 29 ноября 2006 г.	Утверждена работа по созданию сети НАТО Включена возможность обмена информацией в операциях Альянса и улучшения защиты от кибератак [16]
Бухарест, Венгрия 3 апреля 2008 г.	Принят проект по Политике по Киберзащите и развитию вспомогательных структур и органов власти для ее реализации [4]
Страсбург-Кель, Франция / Германия 2-3 апреля 2009 г.	Создан центр управления кибервойной НАТО (CDMA). Улучшение существующей способности реагирования на инцидент с компьютерами. НАТО активизировала совместную киберзащиту Центр передового опыта (CCD COE) в Эстонии [17]

Продолжение табл. на с. 48

Лиссабон, Португалия 20 ноября 2010 г.	К июню 2011 г. Совет призвал обновить политику углубленной киберзащиты НАТО, а также принял поддерживающий план действий Ускоренная цель – способность реагирования на компьютерные инциденты НАТО (NCIRC) до полной функциональной возможности (FOC) к 2012 г. Совет призвал все органы НАТО • находиться под централизованной киберзащитой • использовать процессы планирования обороны НАТО для развития возможностей киберзащиты союзников и улучшения интероперабельности • тесно сотрудничать с другими субъектами, такими как Организация Объединенных Наций (ООН) и Европейский союз (ЕС) [10]
Чикаго, Иллинойс, США 20 мая 2012 г.	Подтверждено принятие новой Концепции, Политики и Плана действий по Кибернетике В Совете НАТО вновь подтвердили усилия по совершенствованию потенциала НАТО и планированию борьбы с кибератаками, продолжая осуществлять централизованную киберзащиту органов НАТО; интегрировать киберзащиту в структуры и процедуры Североатлантического союза и укреплять сотрудничество и взаимодействие Альянса [4]
Ньюпорт, Уэльс, Великобритания 5 сентября 2014 г.	Совет одобрил расширенную политику кибервойны Совет вновь подтвердил предпринимаемые усилия по совершенствованию потенциала НАТО и планированию борьбы с кибератаками посредством новых инициатив с промышленностью; с обучением и упражнениями в области кибервойны; и с возможностями киберпространства [18]
Варшава, Польша 8-9 июля 2016 г.	Альянс сталкивается с рядом проблем и угроз безопасности, которые возникают как с востока, так и с юга; от государственных и негосударственных субъектов; от военных сил и от террористических организаций, кибер-или гибридных нападений Кибератаки квалифицируются как явный вызов безопасности Альянса и могут быть столь же вредными для современных обществ, как и обычная атака Было заявлено: «Мы будем и далее укреплять наши партнерские отношения с другими международными организациями и странами-партнерами, а также с промышленностью и научными кругами через отраслевое киберпартнерство НАТО» Кибербезопасность и информационная безопасность были упомянуты в качестве основных направлений сотрудничества со странами-партнерами (например, Иордания) [19]

Рассматривая документы, можно отметить, как на современном этапе стали меняться основные угрозы для НАТО. Прослеживается процесс переформирования разного вида угроз. Нетрадиционные виды угроз, связанные с киберпространством, во многом видоизменялись и эволюционировали, соответственно менялись и подходы по устранению угроз, что и рассматривается в вышеуказанных документах. После Уэльсского саммита в 2014 г.,

согласно политике НАТО по усиленной политике кибербезопасности, кибероборона была напрямую связана с традиционным назначением НАТО на коллективную оборону. И другое важное решение заключалось в том, что международное право применяется к киберпространству [13].

В целом формирование и развитие киберспособностей НАТО проистекало по традиционному пути – от формального подписания соответствующих соглашений к созданию на их базе организационных структур. В НАТО также есть несколько основных вспомогательных миссий, которые включают общую ситуационную осведомленность в киберпространстве, защиту критической инфраструктуры (CIP), защиту критической информационной инфраструктуры (CIIP), борьбу с терроризмом, поддержку развития киберпотенциала стран-членов и реагирование на кризисы, связанные с киберпространством.

Структура командования НАТО формируется двумя стратегическими командованиями НАТО: Операционное командование союзников и АСТ -Трансформация командования союзников. Ключевое слово названия этого командования – «трансформация», это означает, что целью организации является развитие способности противостояния современным угрозам посредством трансформации. АСТ организован вокруг четырех основных функций: стратегическое мышление; развитие возможностей; образование, обучение и практические учения; сотрудничество и взаимодействие. Эти две командные группы работают вместе, определяя основные векторы работы Альянса.

В то время как АСО (Командные операции союзников) фокусируется на текущих операциях, АСТ концентрируется на инициативах по трансформации военной структуры, сил, возможностей и доктрины НАТО. Из штаб-квартиры в Норфолке, штат Вирджиния, АСТ руководит тремя основными подразделениями: Объединенным центром боевых действий в Штравангере, Норвегия; Центром подготовки совместных сил в Быдгоще, Польша; и Объединенным центром анализа и освоения опыта в Монсанто, Португалия. Другие образовательные и учебные центры НАТО и центры передового опыта (COE) координируют свою деятельность с АСТ [1].

Единственным аккредитованным НАТО Центром передового опыта, посвященным деятельности в киберпространстве, является Центр повышения квалификации кибербезопасности (CCD COE), расположенный в Таллинне, Эстония. CCD COE был создан в октябре 2008 г. с помощью меморандума о взаимопонимании между семью странами НАТО (Эстония, Германия, Италия, Литва, Латвия, Словацкая Республика и Испания) с видением «расширить возможности совместной киберзащиты НАТО и стран НАТО», тем самым улучшая взаимодействие Альянса в области совместной киберзащиты» [5]. Диверсификация деятельности структур киберзащиты, их интеграция в структуры, обеспечивающие противодействие традиционным угрозам, и наличие единого командно-координационного центра намного усилило кибероборону Альянса.

Еще одним доказательством цифровой зависимости военных сил было исследование Лаборатории Касперско-

го по глобальным кибератакам под названием «Неттравеллер», где военная сфера упоминались как одна из наиболее целевых областей [14]. Проводимый анализ развития стратегий кибербезопасности, полученных из анализа документов, предполагает, что стратегии кибербезопасности реагируют на события, и, следовательно, в течение последних пяти лет акцент изменился на наращивание кибервозможностей в военной сфере.

Из обсуждения возможностей киберпространства НАТО вытекают нижеследующие выводы. Институциональное участие НАТО в киберпространстве аналогично другим формам эволюции, которые Североатлантический союз претерпел с момента его образования. После Лиссабонского саммита 2010 г. изменения кибераспектов доктрины НАТО были медленным и не полностью подтвержденным процессом. Отношения между киберпространством и информационными операциями в доктрине оставались неясны. Роль киберпространства в сдерживающих операциях НАТО пока не определена ни на одном открытом форуме. Киберпространство представляет собой сеть со сложными и взаимосвязанными проблемами, такими, как защита критической инфраструктуры на уровне НАТО и на национальном уровне. У НАТО есть хорошо развитая промышленность, страны-партнеры и организации, такие, как ЕС, во многих аспектах связанные с ней по кибердеятельности. НАТО взяла на себя ведущую роль в глобальном масштабе в установлении стандартов для юридической оценки деятельности в киберпространстве.

Проблемы глобального характера, с которыми сталкивается НАТО, подтолкнули Североатлантический союз к пересмотру политики обороны и преобразованию военных структур. Эти изменения привели к обеспечению лидирующих позиций НАТО в области кибербезопасности, а также в воздушной, наземной, морской и космической областях. Динамика дальнейшего развития кибервозможностей НАТО носит разновекторный характер и тенденцию развития многопрофильности кибероборонь Альянса. Вместе с тем неизбежно будет расти и зависимость НАТО от информационных технологий, делая систему обороны более уязвимой. Предусмотреть, изучить и предотвратить различные виды кибер атак намного сложнее, чем традиционные типы угроз. В связи с укреплением НАТО в области кибербезопасности зависимость Альянса от киберпространства возросла.

ИСТОЧНИКИ И ЛИТЕРАТУРА

1. Allied Command Transformation // NATO [official website]. – URL: https://www.nato.int/cps/en/natohq/topics_52092.htm?selectedLocale=en (дата обращения: 10.02. 2018).
2. Bucharest Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008 // NATO [official website]. – URL: https://www.nato.int/cps/en/natolive/official_texts_8443.htm (дата обращения: 10.02.2018).
3. Caton J.L. NATO cyberspace capability: a strategic and operational evolution // Internet Archive [website]. – URL: https://archive.org/stream/NATOCyberspaceCapability/NATO/Cyberspace Capability - A Strategic and Operational Evolution_djvu.txt (дата обращения: 10.02.2018).

4. Chicago Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012 // NATO [official website]. – URL: https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en (дата обращения: 10.02.2018).
5. Centre is the first International Military Organization hosted by Estonia: October 28, 2008 // NATO Cooperative Cyber Defence Centre of Excellence [official website]. – URL: https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html (дата обращения: 10.02.2018).
6. Defending the networks // NATO [official website]. – URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (дата обращения: 10.02.2018).
7. Healey J., van Bochoven L. NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow (27.02.2012) // Atlantic Council [website]. – URL: http://www.atlanticcouncil.org/publications/issue-briefs/natos-cyber-capabilities-yesterday-today-and-tomorrow
8. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World: May 17, 2011 // Public Intelligence [website]. – URL: https://publicintelligence.net/white-house-international-strategy-for-cyberspace/ (дата обращения: 10.02.2018).
9. Jordan B. US Still Has No Definition for Cyber Act of War // Military.com [website]. – URL: https://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html (дата обращения: 10.02.2018)
10. Lisbon Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, November 20, 2010 // NATO [official website]. – URL: https://www.nato.int/cps/en/natohq/official_texts_68828.htm (дата обращения: 10.02.2018).
11. NATO Rapid Reaction Team to fight cyber attack, 13 March 2012 // NATO [official website]. – URL: https://www.nato.int/cps/en/natolive/news_85161.htm (дата обращения: 10.02.2018).
12. NATO Communications and Information Agency [official website]. – URL: http://www.ncia.nato.int/Pages/default.aspx. (дата обращения: 10.02.2018).
13. NATO Summit Updates Cyber Defence Policy, October 24, 2014 // NATO Cooperative Cyber Defence Centre of Excellence [official website]. – URL: https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html (дата обращения: 10.02.2018).
14. NetTraveler: a new cyber-spy campaign is revealed // Kaspersky Laboratory [website]. – URL: https://www.kaspersky.ru/blog/nettraveler/14792/ (дата обращения: 10.02.2018).
15. Prague Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague on 21 November 2002 // NATO [official website]. – URL: https://www.nato.int/docu/pr/2002/p02-127e.htm (дата обращения: 10.02.2018).
16. Riga Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006 // NATO [official website]. – URL: https://www.nato.int/cps/en/natohq/official_texts_37920.htm (дата обращения: 10.02.2018).
17. Strasbourg/Kehl Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg, April 4, 2009 // NATO [official website]. – URL: https://www.nato.int/cps/en/natolive/news_52837.htm (дата обращения: 10.02.2018).
18. Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 5, 2014 // NATO [official website]. – URL: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (дата обращения: 10.02.2018).

19. Warsaw Summit Communiquй Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 // NATO [official website]. – URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (дата обращения: 10.02.2018).

SOURCES AND REFERENCES

1. Allied Command Transformation. NATO [official website]. Available at: https://www.nato.int/cps/en/natohq/topics_52092.htm?selectedLocale=en (accessed: 10.02. 2018).
2. Bucharest Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. NATO [official website]. Available at: https://www.nato.int/cps/en/natolive/official_texts_8443.htm (accessed: 10.02.2018).
3. Caton J.L. NATO cyberspace capability: a strategic and operational evolution. Internet Archive [website]. Available at: https://archive.org/stream/NATOCyberspaceCapability/NATO/Cyberspace Capability – A Strategic and Operational Evolution_djvu.txt (accessed: 10.02.2018).
4. Chicago Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012. NATO [official website]. Available at: https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en (accessed: 10.02.2018).
5. Centre is the first International Military Organization hosted by Estonia: October 28, 2008. NATO Cooperative Cyber Defence Centre of Excellence [official website]. Available at: https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html (accessed: 10.02.2018).
6. Defending the networks. NATO [official website]. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm (accessed: 10.02.2018).
7. Healey J., van Bochoven L. NATO‘s Cyber Capabilities: Yesterday, Today, and Tomorrow (27.02.2012). Atlantic Council [website]. Available at: http://www.atlanticcouncil.org/publications/issue-briefs/natos-cyber-capabilities-yesterday-today-and-tomorrow
8. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World: May 17, 2011. Public Intelligence [website]. Available at: https://publicintelligence.net/white-house-international-strategy-for-cyberspace (accessed: 10.02.2018).
9. Jordan B. US Still Has No Definition for Cyber Act of War. Military.com [website]. Available at: https://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html (accessed: 10.02.2018).
10. Lisbon Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, November 20, 2010. NATO [official website]. Available at: https://www.nato.int/cps/en/natohq/official_texts_68828.htm (accessed: 10.02.2018).
11. NATO Rapid Reaction Team to fight cyber attack, 13 March 2012. NATO [official website]. Available at: https://www.nato.int/cps/en/natolive/news_85161.htm (accessed: 10.02.2018).
12. NATO Communications and Information Agency [official website]. Available at: http://www.ncia.nato.int/Pages/default.aspx. (accessed: 10.02.2018).
13. NATO Summit Updates Cyber Defence Policy, October 24, 2014. NATO Cooperative Cyber Defence Centre of Excellence [official website]. Available at: https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html (accessed: 10.02.2018).
14. NetTraveler: a new cyber-spy campaign is revealed. Kaspersky Laboratory [website]. Available at: https://www.kaspersky.ru/blog/nettraveler/14792/ (accessed: 10.02.2018).
15. Prague Summit Declaration: Issued by the Heads of State and Government participating in the

meeting of the North Atlantic Council in Prague on 21 November 2002. NATO [official website]. Available at: https://www.nato.int/docu/pr/2002/p02-127e.htm (accessed: 10.02.2018).
16. Riga Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006. NATO [official website]. Available at: https://www.nato.int/cps/en/natohq/official_texts_37920.htm (accessed: 10.02.2018).
17. Strasbourg/Kehl Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg, April 4, 2009. NATO [official website]. Available at: https://www.nato.int/cps/en/natolive/news_52837.htm (accessed: 10.02.2018).
18. Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 5, 2014. NATO [official website]. Available at: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (accessed: 10.02.2018).
19. Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. NATO [official website]. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed: 10.02.2018).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Курылев Константин Петрович – доктор исторических наук, доцент кафедры теории и истории международных отношений Российского университета дружбы народов;
e-mail: kuryljov@narod.ru

Цаканян Владимир Тигранович – аспирант, ассистент Российского университета дружбы народов;
e-mail: vladt20@mail.ru

INFORMATION ABOUT THE AUTHORS

Konstantin P. Kurylev – Doctor of Historical Sciences, professor of the Department of the Theory and the History of International Relations, Peoples' Friendship University of Russia;
e-mail: kuryljov@narod.ru

Vladimir T. Tsakanyan – post-graduate student, assistant lecturer, Peoples' Friendship University of Russia;
e-mail: vladt20@mail.ru

ПРАВИЛЬНАЯ ССЫЛКА НА СТАТЬЮ

Курылев К.П., Цаканян В.Т. Цифровая зависимость НАТО // Вестник Московского государственного областного университета. Серия: История и политические науки. 2018. № 1. С. 45–53.
DOI: 10.18384/2310-676X-2018-1-45-53

FOR CITATION

K. Kurylev, V. Tsakanyan. Digital Dependence of NATO. In: *Bulletin of Moscow Region State University.* Series: History and Politic Sciences, 2018, no 1, pp. 45–53.
DOI: 10.18384/2310-676X-2018-1-45-53