ISSN (Print)2616-6887
ISSN (Online) 2617-605X

ВЕСТНИК
ЕВРАЗИЙСКОГО
НАЦИОНАЛЬНОГО
УНИВЕРСИТЕТА
ИМ. Л.Н. ГУМИЛЕВА

BULLETIN
of L.N. GUMILYOV
EURASIAN NATIONAL
UNIVERSITY

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ
УНИВЕРСИТЕТІНІҢ
ХАБАРШЫСЫ

САЯСИ ҒЫЛЫМДАР. АЙМАҚТАНУ. ШЫҒЫСТАНУ. ТҮРКІТАНУ сериясы

POLITICAL SCIENCE. REGIONAL STUDIES. ORIENTAL STUDIES. TURKOLOGY Series

Серия **ПОЛИТИЧЕСКИЕ НАУКИ. РЕГИОНОВЕДЕНИЕ. ВОСТОКОВЕДЕНИЕ. ТЮРКОЛОГИЯ**

№ 1 (130)/2020

1995 жылдан бастап шығады
Founded in 1995
Издается с 1995 года

Жылына 4 рет шығады
Published 4 times a year
Выходит 4 раза в год

Нұр-Сұлтан, 2020
Nur-Sultan, 2020
Нур-Султан, 2020

Редакцияның мекенжайы: 010008, Қазақстан, Нұр-Сұлтан қ., Сәтпаев к-сі, 2, 402 б.
Тел.: +7(7172) 709-500 (ішкі 31-432)
E-mail: vest_polit@enu.kz, web-site:http://bulpolit.enu.kz/
Жауапты хатшы, компьютерде беттеген: Ә.С. Жұматаева

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің хабаршысы.
САЯСИ ҒЫЛЫМДАР. АЙМАҚТАНУ. ШЫҒЫСТАНУ. ТҮРКІТАНУ сериясы
Меншіктенуші: ҚР БҒМ «Л.Н. Гумилев атындағы Еуразия ұлттық университеті» ШЖҚ РМК
Қазақстан Республикасының Ақпарат және коммуникациялар министрлігінде тіркелген. 25.05.18 ж. № 17125-Ж -тіркеу куәлігі
Басуға 30.03.2020 ж.қол қойылды
Ашық қолданудағы электрондық нұсқа: http:// bulphysast.enu.kz
Мерзімділігі: жылына 4 рет. Тиражы: 25 дана
Типографияның мекенжайы: 010008, Қазақстан, Нұр-Сұлтан қ., Қажымұқан к-сі,13/1, тел.: +7(7172)709-500 (ішкі 31-432)

Editorial address: 2, Satpayev str., of. 402, Nur-Sultan city, Kazakhstan, 010008.
Tel.: +7(7172) 709-500 (ext. 31-432). E-mail: vest_polit@enu kz, web-site: http://bulpolit.enu.kz/
Responsible secretary, computer layout: Aliya Zhumatayeva

Bulletin of the L.N.Gumilyov Eurasian National University POLITICAL SCIENCE. REGIONAL STUDIES. ORIENTAL STUDIES. TURKOLOGY Series
Owner: Republican State Enterprise in the capacity of economic conduct «L.N.Gumilyov Eurasian National University» Ministry of Education and Science of the Republic of Kazakhstan
Registered by Ministry of information and communication of Republic of Kazakhstan. Registration certificate No. 17125-Ж from 25.05.2018
Signed in print 30.03.2020. Available at: http:// bulphysast.enu.kz
Periodicity: 4 times a year. Circulation: 25 copies
Address of printing house: 13/1 Kazhimukan str., Nur-Sultan, Kazakhstan 010008; tel.: +7(7172) 709-500 (ext.31-432)

Адрес редакции: 010008, Казахстан, г. Нур-Султан, ул. Сатпаева, 2, каб. 402
Тел.: +7(7172) 709-500 (вн. 31-432)
E-mail: vest_polit@enu.kz, web-site: http://bulpolit.enu.kz/
Ответственный секретарь, компьютерная верстка: А.С. Жуматаева

Вестник Евразийского национального университета имени Л.Н.Гумилева.
Серия:ПОЛИТИЧЕСКИЕ НАУКИ. РЕГИОНОВЕДЕНИЕ. ВОСТОКОВЕДЕНИЕ. ТЮРКОЛОГИЯ
Собственник: РГП на ПХВ «Евразийский национальный университет имени Л.Н. Гумилева» МОН РК
Зарегистрирован Министерством информации и коммуникаций Республики Казахстан
Регистрационное свидетельство № 17125-Ж от 25.05.18 г.
Подписано в печать: 30.03.2020 г.
Электронная версия в открытом доступе: http:// bulphysast.enu.kz
Периодичность: 4 раза в год. Тираж: 25 экземпляров
Адрес типографии: 010008, Казахстан, г. Нур-Султан, ул. Кажымукана, 13/1, тел.: +7(7172)709-500 (вн.31-432)

МАЗМҰНЫ

CONTENTS

СОДЕРЖАНИЕ

ПОЛИТИЧЕСКИЕ НАУКИ

КОЛОНКА РЕДАКТОРА

Политическое воззрение АБАЯ: критический синтез современности

В Казахстане 2020 год ознаменован 175-летним юбилем Абая Кунанбаева – выдающегося мыслителя и поэта, философия которого стала неотъемлемой частью культурной и национальной идентичности гражданского общества в мировом масштабе.

Президент Республики Казахстан Касым-Жомарт Токаев в статье «Абай и Казахстан в XXI веке» призвал осмыслить творческое наследие великого Абая и рационально использовать его в деле модернизации общественного сознания и духовного развития нации. Концепция статьи стала важным компонентом государственной политики Казахстана, направленной на сохранение исторического наследия во имя будущего поколения.

Что может быть общего между жизненными установками, философией, знаниями Абая Кунанбаева XIX века и инновационной современностью XXI века?

Прежде всего отметим концепцию Абая о всесторонне развитом человеке, «Толық адам», в которой заложена идея о человеческом капитале: о трудолюбивых, открытых миру, стремящихся к постоянному развитию и добру граждан общества. Эта концепция в современных условиях становится главным ориентиром в воспитании студенческой молодежи в университетах Казахстана.Что мы должны извлекать из творчества Абая для политической науки? В чем актуальность и особенность политических воззрений Абая?

Обратимся к двум тенденциям политического воззрения Абая.

Во-первых. Эпоха Абая. Из политической истории мы знаем, что на рубеже XIX-XX веков в Казахстане происходили перемены в социально-экономической, политической и культурной сферах жизнедеятельности общества. Влияние капиталистических отношений, развитие демократической мысли, увеличение роли и значимости науки, образования способствовали началу прогресса и пересмотру устоявшихся ценностей, поиску новых ориентиров развития казахстанского общества.

Эпоха Абая - это время патриархально-феодальных устоев в казахской степи, которые стали трансформироваться с появлением товарно-денежных отношений, усилением феодального и колониального гнета, упразднением ханства, установлением волостного правления и вследствие борьбы за власть. В этих условиях политические воззрения и демократические стремления в борьбе за интересы трудового народа у Абая проявляются в его произведениях, отражающих проблемы социально-политической, экономической и культурной жизни общества.

К примеру, мыслитель поднимал вопросы демократизации судопроизводства, классовой сущности системы «выборов», политического союза царских властей и казахской феодальной верхушки в управлении регионами. На должности биев, по мнению Абая, «избираются невежественные люди», не знающие казахского обычного права, сводов законов, созданных Касымханом, Есимханом и Таукеханом.

По своим политическим взглядам Абай был далек от революционного демократизма и понимания необходимости модернизации экономической основы господствовавших общественно-политических порядков. Полагаем, что мыслитель с позиций идеализма считает политическую власть всесильной, так как все происходящее в общественной жизни зависит от воли людей, занимающих высокие государственные посты.

Другим аспектом в произведениях Абая стали идеи о роли общественных условий в формировании характера личности. Он писал: «Человек — дитя своего времени. Если плох тот или иной человек, то в этом виноваты все его современники». В одном из стихотворений 1902 года Абай отмечал: «Эпоха тянет за собой всех. Эпоха формирует людей», однако

рамки патриархально-феодального общества не изменили его идеалистических взглядов на общественную жизнь.

Во-вторых. Эпоха XXI века. В наше время глобальные вызовы и риски требуют переосмысления Абая в современной политической науке. В условиях XXI века мировая цивилизация достигла суперскоростных инновационных технологий, люди стали образованными, креативными, активными участниками всех политических процессов гражданского общества. Однако сохранилась одна тенденция - социальные отношения природы человека, коммуникация между властью и обществом.

В этом аспекте книга наставлений «Гаклия» (Слова-назидания) Абая обретает особую актуальность в осмыслении богатства духовной культуры наших предков, в сохранении идентичности социума в потоке глобализации и социальной ответственности каждого гражданина.

В книге наставлений Абай излагает свое видение истории казахов, человеческого капитала, основанных на вопросах государственного управления, образования, нравственности, языка общения, права и морали. От культурного развития человека, считал мыслитель, напрямую зависит развитие мира. Чем больше узнает человек о мире, тем светлее становятся его душа и мысли. Высоконравственные люди — основа счастливого общества.

Проведем параллель между идеями Абая и актуализацией его концепций в государственной политике Казахстана.

Идеи Абая в **XIX** веке	Актуальность идеи в **XXI** веке
Концепция «полный человек»	Духовная основа человеческого капитала и социальная ответственность
Обучение и развитие народа	Непрерывное образование личности
Изучение иностранных языков	Концепция трехязычья в Казахстане
Уважительное отношение к родному языку	Развитие государственного языка
Изучение искусства	Формирование интеллектуальной нации
Единство народа и миролюбие	Конструктивный диалог между властью и обществом, Национальный совет общественного доверия
Проблема меритократии	Президентский молодежный кадровый резерв – социальный лифт для талантливой молодежи
Создание справедливого общества	Общество Всеобщего Труда Первого Президента Казахстана - Елбасы Н.А. Назарбаева и Концепция «народного государства» Президента РК К.-Ж.Токаева
Понятие «Камиль-мусульманин»	Съезды лидеров мировых и традиционных религий в Казахстане

В 32-ом слове «Слов-назиданий» Абай говорит о важности образования в жизни. К примеру, *«Когда вы изучаете науку, вы должны научиться знать правду, а не использовать свои знания, чтобы вступать в конфликт с кем-либо. Надеясь помнить хорошо то, что ты знаешь, и надеясь, что узнаешь то, что не знал… У человека есть два оружия для развития науки и образования, первое – мышление, обмен мнениями, второе – сохранить и защитить полученные знания»*.

Эти мудрые слова должны стать эталоном для нашей студенческой молодежи: быть гражданами с высокими морально-этическими, культурными и общечеловеческими

ценностями. Вот почему идеи мудрого Абая по-прежнему актуальны.

Полагаем, что Абай, будучи первым евразийцем, призывал не замыкаться лишь в своей культуре, активно учить языки, познавать мировую культуру, обогащать тем самым свои познания об окружающем мире.

Для наших авторов, политологов, международников, тюрколов и регионоведов, есть большой диапазон исследования наследия Абая Кунанбаева в широком поле политической науки.

С уважением, главный редактор,
доктор политических наук,
профессор ЕНУ им. Л.Н. Гумилева
Нуртазина Р.А.

IRSTI 11.01.29

T.A. Kamaljanova, A.Zh. Khussainova
L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan
(E-mail: Takhira.Kamaljanova@mail.ru, asselxus@gmail.com)

The most influential cybercampaigns

Abstract. This article depicts the advancement and future of cyberwar and uncovers an arrangement of politically propelled cyberattacks outlined not as it were to crush military objects but too to disturb essential public infrastructure. The cyber potential of states are highlighted such as Iran, North Korea, and Russia. This article examines the need for legitimate systems characterizing worldwide standards of appropriate and unappropriate hacking exercises and focuses out that cyber weapons should remain under the scrutiny of all country states since these projects include groups of proficient developers and millions of dollars. Apparatuses of cyberwarfare no matter how fantastically modern or the completely simple they ought to be carefully examined in arrange to adjust cybersecurity apparatuses right on time. The work notes that cyberattack such as Stuxnet serves as the starting point for the worldwide cyber arms race. Cyber peace activities are considered as productive as cybersecurity with regard to long-term prospects.

Keywords: Cyberwar, military hacks, consequences for civilians, global cyber arms race, cybersecurity.
DOI: https://doi. org/10. 32523/26-16-6887/2020-130-1-137-144

Introduction. A while ago, our cyberwar dreams were full of terrifying hypothetics about what's going to happen if government-sponsored hackers initiate serious attacks that leave entire cities without electricity and water supply. Or what to do if essential objects like clinics, airports and banks are frozen across a region, for example. And how to measure the economic loss of all chain players in the event of shipping companies, oil refineries so factories being close down?

Technology is making strides too rapidly and as a result science fiction becomes a reality in the context of cyberwar. Taking such events into account, this article aimed to show that the threat of hacking goes further than normal vandalism, criminal speculation and even spying. The paper shows how physical-world disruption can not only be accomplished by military attacks and terrorist sabotages.

Research methods. The field of cyber warfare is certainly a challenge for some ordinary researchers who do not have a technical background while this subject is linked to IT. Nonetheless, by using outlets that describe "easy-to-understand" incidents, we have addressed this problem. Because literature review was the main research methodology in our article, we were attempting to include various perspectives on cyberwar problems.

1.1. Methodology

This paper discusses and analyzes the sequence of cyber attacks that the research community provides. The recent effect of electronic conflicts has been debated in the contemporary world. They summarized and addressed what action should be taken to better address the problem of cyber warfare in future.

During the writing of the scientific article, methods of a theoretical level were used: analysis, synthesis, study and generalization, induction and deduction, comparison, as a method of empirical research, as well as the main provisions of the universal dialectic method.

History. Cyber attack is a strategic way of terrorizing businesses of different sizes and bringing countries into a state of addictivity for some period. History shows that people can accommodate transport scarcity and currency exposure, but how do they embrace situations in

which basic services including power and heat have been denied?

The new super-dangerous cyber attack tactics tend to evolve in the hands of countries like Iran, northern Korea, and Russia, which is of utmost concern. That all suggests the cyber-war threat is just a few steps away.

Hacking is not just a way to increase role, cyber attacks could be a big tactic in the War itself. In 2001, President Bill Clinton clarified this kind of concept of cyberwar when he said that "our vital networks are linked by and operated by machine every day from power structures to air traffic control," and that someone may sit on the same device, pirate in a computer system and probably paralyze a corporation, a town or a country. [1].

Since then, the definition for cyberwar has been developed into one that may have been more clearly set out in Cyber War, a book written in 2010, co-writtenby Richard Clarke, Presidents Bush National Security Adviser, and Robert Knake, former President Obama's cyber-security advisor. Clarke and Knake described cyberwar as "acts by a nation state which infiltrate computers or networks of another nation in order to cause damage or disruption" [2].

Until today, a severe counterpart of a physical assault has indirectly been described as cyberwarfare.

An early example is the well-known cyber espionage program' Moonlight Maze' labeled as Advanced Permanent Maps of military installations, equipment specifications and other sensitive data being copied. The Pentagon tracked the attack back on what was regarded in Russia as a mainframe. [3].

In Estonia, one of the world's most wired nations, another major event concerning Russia in cyberspace took place. The service denial attacks that triggered about two days following the street disruptions left consumers without links to major publications, banks and news media websites. There was a significant lack of access to policy and news media portals because it did not allow government information to be disseminated at a time of crisis. Estonia has no BBC and no CNN office and if all those things fail, it does not have the media system to get news as it is, for instance, in the United Kingdom. More Estonia people are relying on the Web for news so they were unable to monitor their attacks [4].

Russia's denial of collaboration, while both countries have an arrangement on cross-border crime investigation, calls for a diplomatic attribution of assaults. Therein the Tallinn Manual proposal on international law and the modern wars was recognized by a community of law scholars from around the world as important.

Very similarly organized and planned attacks have taken place in Georgia. DDoS attacks targeted 90% of all domain addresses in Gov.ge as well as a significant proportion of the.ge domain addresses. The cyber attacks in Georgia have been carried out, according to this tradition, by patriotic citizens engaged and recruited through social media. xaker.ru and StopGeorgia.ru were the major hacker sites for collaboration and sharing of resources. And hacker groups where more technically knowledged group members supplied the least technologically experienced followers with resources, bugs and goal lists. The Georgian war of 2008 was the first such hybrid conflict were mixed in which traditional armed and hacker powers. The nation is a primary indication of the cyberwar, though, despite the comparatively simple cyber attacks by Russia and Georgia's small percentage of internet users at that point.

Throughout 2010, virtual war's complexity changed forever. It began with the disabling of industrial automatic control systems by Sergey Ulasen, an employee of the VirusBlokAda Security Company in Belarus. It has become apparent that Stuxnet (the codenamed Olympic Games) is a large-scale, rather than simplified operation certainly linked to the contamination of industrial gas centrifuge controls at Iran's nuclear fuel plant in Natanz [5].

Stuxnet struck Iran hardest, according to analysts with the US-based antivirus company Symantec. Around 60% of all infected PCs in that country is found in the earliest known infection [7]. The New York Times reported that Stuxnet was the product of the NSA and Israeli intelli-

gence to hamper Iran's nuclear bomb attempts [8]. After using compromised personal computers and perhaps attackers attacked personal computers of the Natanz workers for the first time, employees of Natanz could have unknownly transported Stuxnet [9].

Start by saying that Iran is one of the most wired in the Middle East–over 70% of Iranians have internet access, suggesting that Iran's cyber capacity is not low [10]. In this case, Stuxnet was deemed a catalyst for the electronic arms race in Iran and a very good excuse. Loud bursts of electronic threats also awoken Tehran.

Among the largest cyber responces conducted by Tehran, were noted such as Madi (2012), Operation Ababil (2012–2014), Operation Shamoon / Operation Shamoon 2 (2012 and 2016–2017), #OpIsrael and #OpUSA (2013 and subsequent years), Operation Cleaver (2012–2014), Operation Saffron Rose (2013–2014), Operation Newscaster (2011– 2014), Operation Wooleen-GoldFish (2014–2015), Operation Wilted Tulip (2013–2017) and Magic Hound (2016–2017). During these activities, dozens of government agencies and private businesses in the countries mentioned above became subjects. For starters, Nicolas Brulez, a leading malware scientist in Kaspersky Lab, said that although the malware was very important in relation to other similar projects, the Madi attackers were able to conduct a continuous surveillance campaign against high-profile victims [11].

Perhaps worth mentioning is another assault by the name of Shamoon. In August 2012, the Saudi-Arabic corporation, Saudi Aramco, was struck with this malware, one of the largest petroleum producers in the world. Data on three quarter of Aramco's business PC's –journals, laptops, communications, photos–were removed, and a burning American flag picture was captured [12].

With respect to Ababil's attack, the volume of traffic flooding at US banks was' multiple times' like Russia had driven Estonia, US government officials and security researchers believed that the assault most likely occurred in reaction to US economic sanctions [13].

Iran has not been alone in harnessing cyber weapons ' capacity worldwide. In this word, North Korea is equivalent to Iran. Experts of the UN also reported that at least 35 groups have operated in North Korea in seventeen nations, including Costa Rica, Gambia, Nicaragua, Kuwait and Liberia. South Korea has no list because this is often the most badly hit nation [14].

Sony, who dared to reveal was first targeted by the intruder before The Interview was published in December 2014. The attacks began with an ominous red-skull photo and a warning, that if unstated demands were not met, the company's "top secrets" would be released. Demands for canceling the release of the comedy in which the North Korean leader Kim Jong-un is murdered by Seth Rogen and James Franco [15]. The stage came when requirements to fail to comply with illegal cyber measures. The most tangible result to date from the hackers, who have been identified as the Guards of Peace, seems to be the twist of five Sony titles, including Fury, Cinderella, Still Alice, Mr. Turner and To Write Love on Her Arms. In spite of this cyber-crime, the FBI publicly identified the government of North Korea as a perpetrator of the attack, based on an overview of the malware compiled on a computer in the Korean language.

The spread of WannaCry could also be seen as an innovation by North Korea. Because the programmer was disabled in Korean even if it is the default language 16]. He or she might have been covering himself. The malware's creator wanted to be unacknowledged because of his innovation to extort money. Kaspersky Lab researchers were certain that the harm caused by that assault could have been avoided if it was not for the persistent use of old computer systems and bad education about the need to upgrade apps. Victims were primarily asked to pay $300-$600, but security researchers alerted consumers that ransom payments should not take place [17]. The assault attacked primarily businesses in the Ukraine, Russia and elsewhere in Europe. But what they tried to achieve in all the political message remains unclear still today.

The level of potential threats on the Internet gives reason to talk about the need for an international treaty, which many call the "digital Geneva Convention", drawing a parallel with The

Hague and Geneva conventions on the laws and customs of war and the protection of its victims [18-3]. In the absence of a treaty and, accordingly, uniform terminology, many technical issues of harmonization of the UN Charter and humanitarian law with the problems of cyber war remain unresolved. At the same time, it is difficult to determine what cyberspace is. Over the years, many attempts have been made to give him a definition (including the official one), but each subsequent one has encountered the need to take into account the dynamics of its development.

States have different priorities in cyberspace. The technologies that provide the "freedom" of the Internet are considered by many countries as a means of cyber attacks, and the technologies and (political and legal) mechanisms to counteract such "freedom" are regarded as a means of ensuring political stability. States such as Russia and the People's Republic of China assess the model of the behavior of the Wild West promoted by the USA in cyberspace as an attempt to instill "wild" values. Countries opposing US dominance in setting standards in cyberspace point to the discovery of digital espionage by the US National Security Agency and the development of cyber warfare by the Pentagon.

The leading countries in the field of information technology - the United States, Russia and China - may be interested in more time to develop their capabilities in cyberspace, to identify their own strengths and weaknesses before concluding an international agreement that can limit their potential. Such an agreement (probably) will not only prohibit offensive cyber operations, but will also limit the subsequent development of cyber warfare tools by analogy with the nuclear non-proliferation regime.

A bilateral agreement between the United States and China on the prohibition of state participation in cybercrime and commercial espionage is the best that could be achieved so far.

D. Abeba points to external, international factors affecting potential models of international and national regulation. Among them he distinguishes: international law; opportunities in the information environment, strategic interests, foreign policy goals of members of the international community (potential opponents), as well as a number of non-governmental organizations; the practice of paramilitary and technology companies involved in the field of information security [19-1].

Factors such as budgets and incentives for potential opponents, although relatively (given the effective use of small investments by Russia and China), can also be considered as influencing regulation.

D. Hollis expresses doubt about the ability of international law to normalize cognitive interaction. In this regard, responsibility not in the military and legal spheres, but in the sphere of production of technologies (codes and algorithms) can become the first line of defense. The complexity and diversification of cyber operations makes it impossible for a uniform legal form. Different contexts require different, including hybrid, legal remedies.

However, it is obvious that the effectiveness of counteracting cyber attacks can be achieved only with an integrated approach to solving this problem.

A cyberattack, as noted earlier, unlike the usual spread of viruses, is targeted and its purpose is the specific system that certain users work with, so it is quite difficult to defend against it.

However, it must be said thet the role of users in preventing cyber attacks is huge, because many computer security incidents become possible precisely because of their fault (using outdated software, switching to unknown external resources, etc.). In order to minimize the risk of cyber attacks on the security of a computer system, the user must comply with the basic rules of cybersecurity.

These rules are a set of forensic preventive knowledge formed on the basis of the analysis of modern incidents of cyberattacks:

One must use only licensed software with the possibility of timely updates. Even large companies often use pirated versions of software. It would seem that this is due to economy of the budget of the organization. However, it is necessary to soberly assess risks. The damage that can

be caused by a cyber attack is disproportionate to the money saved on licensed software;

It is necessary to monitor the relevance of antivirus programs;

One cannot follow external links received from unknown users;

It is recommended to delete unread suspicious emails from unknown users. Once opened it, do not follow the links to unknown resources indicated in it, do not open or download attachments;

Do not use electronic storage media in unknown devices and vice versa;

It is advisable to regularly back up files to external media that is not permanently connected to the computer system. If attackers encroach on these systems, you can always continue to work with the backup;

It is recommended not to use the same password for different applications, and also not to use personal data as a password;

If the computer system was still attacked, do not rush to transfer money to the attackers, since there is no guarantee that the malicious software will be permanently deleted from the computer and the extortion will not be repeated again, and also not to hide the computer security incident, as from the manual, so from law enforcement, do not try to reinstall the system yourself. It is necessary to immediately inform law enforcement agencies and take all measures to preserve and fix the traces of the cyber attack.

Compliance with the rules presented will protect the computer system of a specific user, will have a significant role in strengthening the information security of the world as a whole, and will also help in fixing traces and in investigating such incidents.

Conclusion. Global powers are poised for the battle. Cyber conflict would probably be described as a modern "Bellum omnium contra omnes" or "the war of all against all" because real intentions are so obscure, while inquiry is carried out in a perfect way.

Today, the main issues on the discussion agenda before the world community should be the development of rules governing the conduct of aggressive actions in "cyberspace." This problem needs to be resolved as soon as possible, since the created samples of cyber weapons are distinguished by global reach, almost instantaneous impact without any way of receiving a warning about its use. Such characteristics make it possible to equate it with strategic offensive weapons, but the development and use of cyber weapons is not limited to any international agreement. The confrontation and rivalry of states and non-state actors in cyberspace is already ongoing, although it would be incorrect to call this a war from a scientific and international legal point of view. Obviously, it is necessary to develop a unified doctrine for responding to threats of this type associated with the use of cyberspace for aggressive purposes.

Despite the magnitude of cyber threats, with the coordination of actions, it is possible to successfully counteract them. If the state is fighting legislative and organizational measures against cybercriminals, then each user can make an invaluable contribution to the common cause - to know and comply with the basic rules of cybersecurity, timely and competently responding to malfunctions in the operation of a computer system.

References

1. Public Papers of the Presidents of the United States. [Electronic resource].- URL: https://www.govinfo.gov/content/pkg/PPP-2000-book1/html/PPP-2000-book1-doc-pg13-2.htm (қаралған күні: 10.01.2020).

2. Greenberg A. The WIRED Guide to Cyberwar. [Electronic resource]. - URL: https://www.wired.com/story/cyberwar-guide/ (қаралған күні: 10.01.2020).

3. Rid T. Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5–32 (2012).

4. Leyden J. Cyberwarriors on the Eastern Front: In the line of fire packet floods. [Electronic resource]. - URL:https://

www.theregister.co.uk/2011/04/25/estonia_cyberwar_interview/ (қаралған күні: 5.12. 2019)
5. Rid T. "Cyber Fail", The New Republic. [Electronic resource]. - URL: https://newrepublic.com/article/112314/obama-administrations-lousy-record-cyber-security (қаралған күні: 5.12. 2019)
6. Keizer G. Iran confirms massive Stuxnet infection of industrial systems [Electronic resource]. - URL: https://www.computerworld.com/article/2516028/iran-confirms-massive-stuxnet-infection-of-industrial-systems.html (қаралған күні: 5.12.19).
7. David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran [Electronic resource]. - URL: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (қаралған күні 5.12. 2019).
8. Albright D. Brannan P. and Walrond C. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment [Electronic resource]. - URL: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (қаралған күні: 5.12. 2019).
9.I Ashish K.S. Iran's growing cyber capabilities in a Post-Stuxnet Era [Electronic resource]. - URL:https://www.atlanticcouncil.org/blogs/new-atlanticist/iran-s-growing-cyber-capabilities-in-a-post-stuxnet-era/ (қаралған күні: 5.12. 2019).
10. Leyden J. New 'Madi' cyber-espionage campaign targets Iran AND Israel [Electronic resource]. - URL:https://www.theregister.co.uk/2012/07/17/madi_cyber_espionage_campaign/ (қаралған күні: 25.12. 2019).
11. Perlroth N. In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. [Electronic resource]. - URL:https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html (қаралған күні: 15.12. 2019)
12. Perlroth N. Quentin Hardy, Bank Hacking Was the Work of Iranians, Officials Say [Electronic resource]. - URL:https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html (қаралған күні: 11.12. 2019)
13. Publication of Infosecurity Magazine. Iran's Operation Saffron Rose Points to Increasing Cyber-Espionage Sophistication [Electronic resource]. - URL: https://www.infosecurity-magazine.com/news/irans-operation-saffron-rose-points-to-increasing/ (қаралған күні: 15.12. 2019).
14. Dong G.L. Cyber Attacks Are North Korea's New Weapon of Choice [Electronic resource]. - URL: https://nationalinterest.org/blog/korea-watch/cyber-attacks-are-north-koreas-new-weapon-choice-87526 (қаралған күні: 25.12. 2019)
15. Luckerson V., Everything We Know About the Massive Sony Hack [Electronic resource]. - URL: https://time.com/3612132/sony-hack-north-korea-interview/ (қаралған күні: 15.12. 2019).
16. Mimosa M., Metadata Analysis Draws its Own Conclusions on WannaCry Authors [Electronic resource]. - URL :https://threatpost.com/metadata-analysis-draws-its-own-conclusions-on-wannacry-authors/126287/ (қаралған күні: 23.12. 2019).
17. Gibbs S., WannaCry: hackers withdraw £108,000 of bitcoin ransom. [Electronic resource]. - URL: https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom (қаралған: күні 5.12. 2019)
18. Singer P., Friedman A. Cybersecurity and cyberwar: What everyone needs to know. – Oxford: Oxford univ. press, 2014. – 320 p.
19. Abebe D. Cyberwar, international politics and institutional design // The university of Chicago law review. - Chicago, 2016.-- Vol. 83, N 1. - P. 1–22.

Т.А. Камалджанова, А.Ж. Хусаинова
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан

Ең ықпалды кибер-науқандар

Аннотация. Бұл мақалада киберсоғыс эволюциясы мен болашағы сипатталған. Әскери объектілерді жою үшін ғана емес, сонымен қатар маңызды азаматтық инфрақұрылымды бұзу үшін жасалған саяси негізделген кибершабуылдардың тізбегі көрсетілген. Иран, Солтүстік Корея және Ресей сияқты мемлекеттердің кибер әлеуеті ерекше атап өтілді. Бұл мақалада хакерлік іс-әрекеттің жаһандық нормаларын анықтайтын заңнамалық базаның жоқтығы талданған. Киберқару барлық мемлекеттердің назарынан тыс қалмауы мақсатымен кәсіби жобалаушылар командасы мен миллиондаған доллар қатысуы дәлел ретінде келтірілген. Киберқару құралдарының қаншалықты күрделі немесе қарапайым болуына қарамастан, киберқауіпсіздік құралдарын дер кезінде бейімдеу үшін әрі қарай зерттелуі керек. Бұл жұмыста Stuxnet сияқты кибершабуыл ғаламдық киберқару жарысының басталуы ретінде қарастырылған. Кибербейбітшілік бастамалары киберқауіпсіздік сияқты ұзақ мерзімді перспективалар үшін тиімді болып саналады.

Түйін сөздер: киберсоғыстар, әскери бұзу шаралары, бейбіт тұрғындарға тигізетін зардаптар, ғаламдық киберқару жарысы, киберқауіпсіздік.

Т.А. Камалджанова, А.Ж. Хусаинова
Евразийский национальный университет им. Л.Н. Гумилева, Нур-Султан, Казахстан

Самые влиятельные кибер-кампании

Аннотация. Эта статья описывает эволюцию и будущее кибервойны, а также раскрывает серию политически мотивированных кибератак, предназначенных не только для уничтожения военных объектов, но и для разрушения важной гражданской инфраструктуры. Рассмотрен киберпотенциал таких стран, как Иран, Северная Корея и Россия. В работе поднимается вопрос отсутствия правовых рамок, определяющих глобальные нормы допустимой и недопустимой хакерской деятельности, а также указывается, что кибероружие заслуживает особого внимания со стороны всех национальных государств, поскольку в этих проектах участвуют команды профессиональных разработчиков и задействованы миллионы долларов. Инструменты кибервойны, какими бы невероятно изощренными или абсолютно простыми они ни были, должны быть тщательно исследованы для того чтобы своевременно адаптировать инструменты кибербезопасности. В статье отмечается, что кибератака, такая как Stuxnet, служит стартовым выстрелом для глобальной гонки кибервооружений. Инициативы по кибермиру считаются эффективными в отношении таких долгосрочных перспектив, как кибербезопасность.

Ключевые слова: кибервойна, военные взломы, последствия для гражданского населения, глобальная гонка кибервооружений, кибербезопасность.

References

1.Public Papers of the Presidents of the United States [Electronic resource]. Available at: https://www.govinfo.gov/content/pkg/PPP-2000-book1/html/PPP-2000-book1-doc-pg13-2.htm (Accessed: 10.01.2020)
2. Greenberg A, The WIRED Guide to Cyberwar [Electronic resource]. Available at: https://www.wired.com/story/cyber-war-guide/ (Accessed: 10.01.2020)
3. Rid T. Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5–32 (2012).
4. Leyden J, Cyberwarriors on the Eastern Front: In the line of fire packet floods [Electronic resource]. Available at :https://www.theregister.co.uk/2011/04/25/estonia_cyberwar_interview/ (Accessed: 5.12. 2019)
5. Rid T, “Cyber Fail”, The New Republic [Electronic resource]. Available at: https://newrepublic.com/article/112314/obama-administrations-lousy-record-cyber-security (Accessed: 5.12. 2019)
6. Keizer G. Iran confirms massive Stuxnet infection of industrial systems [Electronic resource]. Available at: https://

www.computerworld.com/article/2516028/iran-confirms-massive-stuxnet-infection-of-industrial-systems.html (Accessed: 5.12. 2019).
7. David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran [Electronic resource]. Available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (Accessed: 5.12. 2019)
8. Albright D., Brannan P, and Walrond C. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment [Electronic resource]. Available at: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (Accessed: 5.12. 2019).
9.I Ashish K.S. Iran's growing cyber capabilities in a Post-Stuxnet Era. [Electronic resource]. Available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/iran-s-growing-cyber-capabilities-in-a-post-stuxnet-era/ (Accessed: 5.12. 2019).
10. Leyden J. New 'Madi' cyber-espionage campaign targets Iran AND Israel [Electronic resource]. Available at: https://www.theregister.co.uk/2012/07/17/madi_cyber_espionage_campaign/ (Accessed: 25.12. 2019).
11. Perlroth N. In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back [Electronic resource]. Available at:https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html (Accessed: 15.12. 2019).
12. Perlroth N. Quentin Hardy, Bank Hacking Was the Work of Iranians, Officials Say [Electronic resource]. Available at:https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html (Accessed: 11.12. 2019).
13. Publication of Infosecurity Magazine. Iran's Operation Saffron Rose Points to Increasing Cyber-Espionage Sophistication [Electronic resource]. Available at: https://www.infosecurity-magazine.com/news/irans-operation-saffron-rose-points-to-increasing/ (Accessed: 15.12. 2019).
14. Dong G.L., Cyber Attacks Are North Korea's New Weapon of Choice. [Electronic resource]. Available at: https://nationalinterest.org/blog/korea-watch/cyber-attacks-are-north-koreas-new-weapon-choice-87526 (Accessed: 25.12. 2019).
15. Luckerson V., Everything We Know About the Massive Sony Hack [Electronic resource]. Available at: https://time.com/3612132/sony-hack-north-korea-interview/ (Accessed: 15.12. 2019).
16. Mimosa M., Metadata Analysis Draws its Own Conclusions on WannaCry Authors [Electronic resource]. Available at:https://threatpost.com/metadata-analysis-draws-its-own-conclusions-on-wannacry-authors/126287/ (Accessed: 23.12. 2019).
17. Gibbs S., WannaCry: hackers withdraw £108,000 of bitcoin ransom [Electronic resource]. Available at: https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom (Accessed: 5.12. 2019)
18. Singer P., Friedman A. Cybersecurity and cyberwar: What everyone needs to know. – Oxford: Oxford univ. press, 2014. – 320 p.
19. Abebe D. Cyberwar, international politics and institutional design // The university of Chicago law review. - Chicago, 2016.-- Vol. 83, N 1. - P. 1–22.

Авторлар туралы мәлімет:

Хусаинова А.Ж. – халықаралық қатынастар кафедрасының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қ.Сәтбаев көш., 2, Нұр-Сұлтан, Қазақстан.

Қамалджанова Т.А. – тарих ғылымдарының кандидаты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қ. Сәтбаев көш., 2, Нұр-Сұлтан, Қазақстан.

Khussainova A. Zh. – Master's student, Department of International Relations, L.N. Gumilyov Eurasian Nation MNational University, Satpayev str.2, Nur-Sultan, Kazakhstan.

Kamalzhanova T.A. – Candidate of Historical Sciences, Associated Professor, Department of International National University, Satpayev str.2, Nur-Sultan, Kazakhstan.