http://ejournal.seaninstitute.or.id/index.php/Ekonomi
Jurnal Ekonomi, Volume 12, No 02, 2023
ISSN: 2301-6280 (print) ISSN: 2721-9879 (online)

CYBERSECURITY ANALYSIS IN THE CONTEXT OF THE RUSSIA-UKRAINE CONFLICT: CHALLENGES, THREATS, AND DEFENSE STRATEGIES

[1]Imam Budiman, [2]Arliya Fadya Salsabila, [3]Chandra Izat Mubarok, [4]Naura Fasya Rustiawan, [5]Rinaldi Anwar Zulfikar
[1,2,3,4,5] Pasundan University , Bandung, Indonesia

ARTICLEINFO

Keywords:
Cyber Security,
Cyber Crime,
Russia-Ukraine,
Securitization

ABSTRACT

The role of cybersecurity in the context of the conflict between Russia and Ukraine has become a concern for the international community due to its widespread impact on national security and regional stability. Cyber attacks have become a significant tool in modern conflicts, and this research aims to understand the role of cybersecurity in the escalation of the conflict between Russia and Ukraine. The role of cybersecurity in this conflict involves cyber attacks carried out by Russia against Ukraine's critical infrastructure. These attacks include targeting Ukraine's communication, power, and financial systems. These attacks have had a significant impact on Ukraine's ability to resist Russian invasion and maintain their national security. Additionally, this paper discusses Ukraine's efforts to strengthen their cyber defense in response to the cyber attacks by Russia. Steps taken by Ukraine include enhancing their cyber defense capabilities, cooperation with international partners, and increasing public awareness of cyber threats. This paper also analyzes the international community's response to cyber attacks in the context of the Russia-Ukraine conflict. International organizations such as NATO and the European Union play a crucial role in providing support and technical assistance to Ukraine in combating cyber attacks by Russia. However, the challenges faced in addressing the evolving cyber threats require stronger cooperation among countries worldwide.

E-mail:

1. INTRODUCTION

The development of time from era to era continues to undergo changes, and advancements in science and technology (S&T) bring various influences and complexities to human life and international relations. The inception of communication patterns through the virtual world or the internet began when the Advanced Research Projects Agency (ARPA) developed a computer network which is now known as the internet.

The birth of the internet eliminated conventional boundaries that were previously adhered to and governed by international consensus. Currently, we have entered the era of Society 5.0, where human life depends on technology to the extent that technology becomes a part of human beings themselves. This has led to a high demand for internet usage in human life, and sectors such as banking, information, and governance now rely on internet networks to be easily accessible to the public.

This also affects the current trend of warfare. In the past decade, the issue of cyber warfare has gained attention and can trigger conflicts between countries, posing a threat to global peace. The head of the United Nations' telecommunications agency, Toure Hamadoun, warned that a world war could occur in cyberspace.

In the context of global conflict, attention to cybersecurity becomes more significant, especially in the situation of the conflict between Russia and Ukraine. The Russia-Ukraine conflict has created complex security challenges and involves crucial aspects of cybersecurity.

The Russia-Ukraine conflict has involved both conventional and non-conventional elements, including significant cyber attacks. These cyber attacks have various objectives, ranging from espionage, data theft, sabotage of critical infrastructure, to the dissemination of propaganda. In the Russia-Ukraine conflict, according to records from the CyberPeace Institute, Ukraine has suffered a total of 280 cyber attacks from January 2022 to February 2023. In the same period, Russia recorded 183 attacks. In a more

comprehensive report, the CyberPeace Institute explains that the attacks Ukraine received include DDoS, malware, phishing, hack and leak, wiper, ransomware, and unidentified attacks.

Reflecting on this, several countries have already established specialized cyber force units for the defense and security of their nations. These agencies or organizations are responsible for coordinating all defense efforts and counterattacks against cybersecurity threats in the virtual world and its network systems. Recognizing the power and potential threats resulting from information technology advancements, many countries are now building their cyber armed forces.

2. METHODS

In the research on cyber security issues arising in Ukraine due to the Russia-Ukraine war, this study employs a descriptive-qualitative research method using a literature review based on existing data, such as books and references. As a result of the war between Russia and Ukraine, Ukraine has suffered losses with the occurrence of system breaches and major cyberattacks on Ukrainian banks, suspected to be caused by Russia. This research aims to analyze how cyber security poses a threat to Ukraine in the midst of the ongoing war between Russia and Ukraine.

3. LITERATURE REVIEW

Securitization Theory

In the book "Security: A New Framework of Analysis" by Buzan, Waever, and Jaap de Wilde, it is explained that security involves actions that go beyond the general rules of framing an issue, whether it falls within the realm of politics or exceeds it. Securitization, on the other hand, is an extreme form of political effort.

Security is usually associated with inter-state warfare in pursuit of interests commonly referred to as traditional security. However, security is no longer limited to traditional security alone, which was predominantly dominated by military forces. The expansion of security now includes non-traditional security, marked by the end of the Cold War, leading to the transformation of security, the expansion of actors, and international security issues.

Threats to security, which were previously concerned with war and nuclear threats, now also include threats to the economy, society, and culture. This is evident in the case of Russia-Ukraine, where the previous traditional security threat of invasion by Russia led to a prolonged war. Currently, Ukraine also faces non-traditional security threats from Russia, particularly in the form of cyber security.

National security, which previously focused on defending the state against physical conditions, now also requires defense through networks due to the advancing digital era. The advancement of digitalization today makes Ukraine need to be wary of hackers who can attack and access sensitive state data, allowing Russia to identify Ukraine's vulnerabilities and potentially leading to Ukraine's defeat in the ongoing war.

Cyber Crime Theory

Cyber attacks are crimes committed by individuals or groups using information technology with the internet as their tool. Cybercrime is a widely used term to describe criminal activities using computer or internet media, as stated by Murti (2005). Security in the form of digital systems poses numerous possibilities for hackers to gain unauthorized access, manipulate, or steal important and confidential data that should not be known by others. In ensuring the confidentiality of a nation's interests, information security requires cyber security with the concepts of confidentiality, integrity, and availability.

The invasion by Russia on Ukraine has resulted in ongoing issues that extend beyond the military domain. Cyber attacks carried out by suspected Russian hackers targeting Ukraine's systems have inflicted damage on Ukraine. The cyber warfare inflicted on Ukraine by Russia serves as an alternative after the military aggression by Russia against Ukraine. By utilizing the internet to attack and breach Ukraine's systems, Ukrainian cyber security is compromised, leading to the exposure of state secrets and undermining the confidentiality, integrity, and availability of information that should have remained secure and protected from adversaries, thus causing harm to the society.

4. RESULT AND DISCUSSION

Cybercrime and Its Threats to Ukraine in the Current Era of Digitalization

In the current era of globalization, technology is widely used by almost all segments of society for communication purposes, both domestically and internationally. Advanced technology has undoubtedly facilitated our lives. However, technological advancements also have negative implications. The sophisticated technology available today has unfortunately become a tool for criminals to commit

cybercrimes, which harm communities. Cybercrime refers to criminal activities carried out through computer networks and the internet, involving hacking and stealing of data and financial information.

Ukraine is a country that has experienced significant losses due to the ongoing conflict with Russia. The conflict between Russia and Ukraine has caused substantial damage to both parties involved. However, in the digital age, the battle extends beyond the physical realm, as digitalization has enabled Russia to launch cyber attacks on Ukraine. The cyber attacks inflicted on Ukraine further exacerbate the panic caused by Russia's military aggression.

The United States Cybersecurity and Infrastructure Security Agency (CISA) has issued warnings regarding the widespread cyber threats posed by Russia. The hacking of Ukrainian government systems and banks has resulted in numerous Ukrainian websites being filled with junk data, rendering them inaccessible. Two of Ukraine's largest banks, Privatbank and Sberbank, have been affected. The hacking activities are suspected to be carried out by Russia, as the hackers' tools used against Ukraine, such as Distributed Denial of Service (DDoS), are supported by Russia. These attacks on Ukraine by Russia emphasize the need for Ukraine to pay closer attention to its national security, not only in terms of military attacks but also in the virtual world. The daily reliance on digitalization has made it easier for Russia to pursue its interests by attacking Ukraine.

In terms of societal security, governments need to be cautious in protecting the rights of their citizens. The cyber attacks suffered by Ukraine require special attention, as the ongoing conflict involves not only military actions but also cyber warfare. In the digital era, attackers find it easier to access and compromise systems, using the internet to obtain sensitive information of their adversaries, which puts the citizens of Ukraine at risk.

Cybersecurity Policies Implemented in Ukraine and Russia

Cybersecurity threats often transcend national borders, and cyber attacks on critical infrastructure in one country can have an impact on the entire European Union (EU). EU member states need to have strong governmental bodies overseeing cybersecurity within their countries and work together with partner countries by sharing information. In late 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented the EU's cybersecurity strategy. The strategy focuses on securing essential services such as energy networks and emphasizes the development of measures to respond to major cyber attacks. It also emphasizes global cooperation to ensure cybersecurity and stability in the digital world. Ukraine has experienced a cyber attack that disrupted its telecommunications infrastructure. In response, Ukraine has increased its cybersecurity workforce by around two-thirds between 2015 and the present. Such investments have contributed to Ukraine's cyber defense during times of war. The global IT industry, in general, has provided ample evidence of Ukraine's readiness to confront and mitigate cyber attacks. An example of this is the large-scale cyber attack originating from Russia against the Ukrainian government's banking sites.

The main provision of Ukraine's constitution (Law, 28.06.1996 № 254к/96-ВР) states, "Protection of Ukraine's sovereignty and territorial integrity, economic and informational security are the most important functions of the state, concerning all Ukrainian citizens." Although cybersecurity is not explicitly mentioned, information security is considered an essential aspect of protection. A closer normative reference to cybersecurity can be found in the Law "On the Fundamentals of National Security of Ukraine" (Law, 19-06-2003 № 964-IV). It lists several main areas of threats to

Cybersecurity Policies Implemented in Ukraine and Russia

The threat of cybersecurity breaches transcends national borders, and cyber attacks on critical facilities in one country can affect the entire European Union (EU). EU member states need to have strong governmental bodies overseeing cybersecurity within their countries and work together with other member states by sharing information. In late 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented the EU's cybersecurity strategy. The strategy includes securing essential services such as energy networks and focuses on building resilience to respond to major cyber attacks. It also emphasizes working with global partners to ensure cybersecurity and stability in the digital world.

Ukraine has experienced cyber attacks that have disrupted its telecommunications infrastructure. As a response, Ukraine has increased its cybersecurity workforce by around two-thirds between 2015 and the present. Such investments may have contributed to Ukraine's cyber defense during times of war. There is substantial evidence that the global IT industry, in general, and the IT community in Ukraine, in

particular, are better prepared to face damaging cyber attacks. An example of this is the large-scale cyber attack originating from Russia against the Ukrainian government's banking sites.

The primary provision of Ukraine's constitution (Law, 28.06.1996 № 254к/96-BP) in Article 17 states, "Protection of Ukraine's sovereignty and territorial integrity, economic and informational security are the most important functions of the state, concerning all Ukrainian citizens." While cybersecurity is not explicitly mentioned, information security is considered a vital aspect of protection. It can be assumed that cybersecurity falls under the realm of information security. The closest normative source to cybersecurity is the Law "On the Fundamentals of Ukraine's National Security" (Law, 19-06-2003 № 964-IV). The law lists several main areas of threats to national security and national interests. These nine areas include External Political Affairs, Military and Border Security, State Security, Social and Humanitarian Affairs, Economy, Civil Defense, Information, Science, and Technology. Threats related to information security are covered under this law, such as the disclosure of state secrets or other prohibited information crucial for protecting national interests, computer crimes, computer terrorism, and the dissemination of false information. The law clearly includes cybersecurity within the field of information security.

The role of cybersecurity in addressing cybercrime to achieve national information resilience is crucial

In the modern era, the advancement of science and technology has led to the emergence of new risks, including cybercrime. In the era of Society 5.0, where in 2022 the International Telecommunication Union (ITU) recorded that the number of active internet users worldwide reached 5.5 billion, which means that 66% of the world's population actively uses the internet. Cybercrime can have various negative impacts, such as the destruction of a country's economy, leakage of sensitive national information, disruption of social order in society, and can be used as a medium for spreading propaganda by radical groups to promote their deviant ideologies.

One of the most prevalent and damaging cybercrimes is ransomware. Ransomware is a type of malicious software or malware that threatens victims by destroying or blocking access to critical data or systems until a ransom is paid. Historically, most ransomware targeted individuals, but lately, human-targeted ransomware attacks on organizations have become increasingly widespread and challenging to prevent and mitigate. Between 2022 and the second quarter of 2022, the global volume of ransomware attacks peaked in the first quarter of 2021, with a total of 189.9 million attacks.

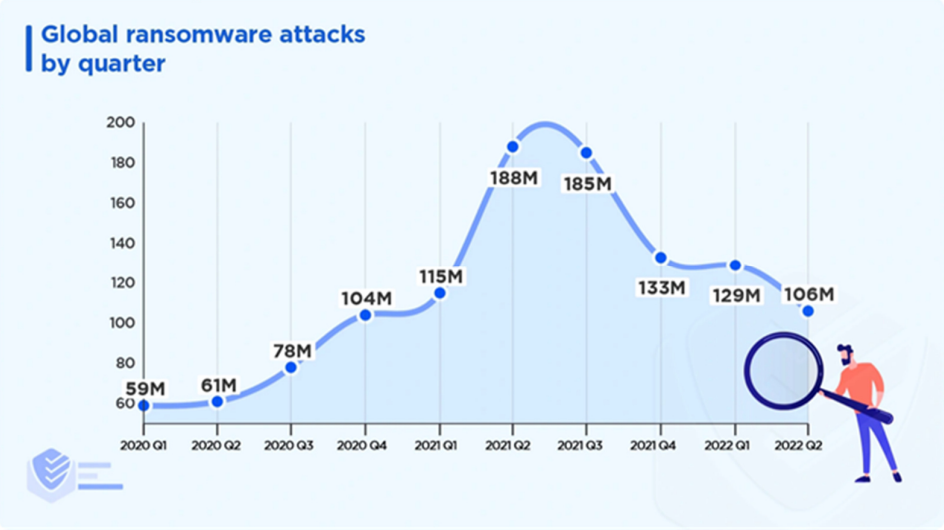

Figure 1. Global Ransomeware attacks by quarter

Cyberattacks can have a significant impact on various critical infrastructures of a country, such as healthcare services, banking, public services, transportation, and government systems. The effects of these attacks are difficult to predict because cyber threats evolve and adapt over time. Here are some recent cyberattacks:

a. In March 2022, the postal system in Greece fell victim to a ransomware attack. The attack disrupted mail delivery and affected financial transactions temporarily.

b. One of India's largest airlines experienced a ransomware attack in May 2022, leading to flight delays, cancellations, and inconvenience for hundreds of passengers.
c. In February 2023, government, parliament, and banking websites in Ukraine were hit by a wave of Distributed-Denial-of-Service (DDoS) attacks. Local research laboratories detected the presence of data-wiping viruses or malware, impacting the functionality of these websites.
d. In May 2021, a US fuel pipeline shut down its services to prevent further breaches after a ransomware attack compromised thousands of employee personal records. This incident caused fuel prices to spike along the East Coast.
e. A German chemical distribution company experienced a ransomware attack in April 2021. Over 6,000 individuals' birthdates, social security numbers, SIM numbers, and some medical data were stolen.
f. One of the world's largest meat suppliers became a target of a ransomware attack in May 2021. After temporarily shutting down its website and halting production, the company ultimately paid an $11 million ransom in Bitcoin.

Mitigation and preventive measures against cybercrime are crucial to protect information systems, including both software and hardware components. In the recent conflict between Russia and Ukraine, Western leaders explicitly stated that they would not send military forces to engage in combat in Ukraine. However, in the digital realm, Western government, military, and commercial actors directly engage in cyberattacks against Russia and assume responsibility for defending Ukraine's networks and data.

The strategic context indicates that despite Ukraine's experience in defending against Russian cyberattacks and its highly skilled experts in protecting critical targets, it may ultimately be unable to prevent significant damage and exploitation of Ukraine's digital networks and data. Ukraine's operational capabilities would be outmatched by Russia's strategic advantage, given its possession of some of the most potent offensive cyber capabilities in the world. As a next step in their efforts to defend national information resilience, Ukraine seeks international partnerships with friendly nations and investments from companies to enhance their cybersecurity defenses.

Cyber Security and the Security of Ukrainian Banks in the Context of the Russia-Ukraine Invasion

The conflict between Russia and Ukraine has brought about various impacts not only on economic, political, and intergovernmental cooperation aspects but specifically on Cyber Security. A series of cyber attacks took down the websites of the Ukrainian military, the Ministry of Defense, and major banks. Cyber Security has become a concern in International Relations due to the significant changes it has caused.

Russian cyber attacks continued until February 24, 2022, concurrent with Russia's military invasion of Ukraine. These attacks targeted Ukraine's communication systems and satellites one hour before the invasion. Russia launched a malware attack called "IsaacWiper" with the aim of blocking access to financial and energy services and detaining refugees trying to enter Romania. These cyber attacks continued until May 2022, leading to a rush of citizens withdrawing money and causing panic and uncertainty.

As a response, Ukrainian Deputy Prime Minister Mykhailo Fedorov established the "IT ARMY" as a preventive measure and to launch counterattacks against Russia. The IT ARMY's targets are the websites of 31 Russian businesses, banks, and government institutions. At least six European Union countries have sent cybersecurity experts to Ukraine. Facebook and Google blocked and banned the monetization of videos and information from Russia. Elon Musk's Starlink service was activated to support recovery operations and cyber attacks. NATO's role in the case of Russia's invasion and cyber attacks that paralyzed the banking sector, government websites, and other institutions has become one of their main missions in the principle of collective defense. This indicates that NATO can intervene to assist Ukraine in the cyber attacks launched by Russia. However, it ultimately depends on the member countries and their decisions to help Ukraine. Apart from a few countries willing to provide assistance to Ukraine, the limited capabilities also pose a challenge in countering cyber attacks due to Russia's expertise and their denial of the cyber attacks they have conducted. Additionally, cyber attacks are often difficult to predict in terms of their timing.

Ukraine's Cybersecurity continues to prepare itself through various measures. Firstly, monitoring and studying patterns of cyber attacks, such as the HermeticWiper malware (2022) and NotPetya (2017). Secondly, the Ukrainian Cyber Agency has issued recommendations to all institutions in the country, both government and private, to review their cybersecurity guidelines and promptly respond to cyber incidents. Thirdly, Ukraine is continuously enhancing international political diplomacy to reduce further escalation.

Overall, the translation above provides an overview of the situation regarding Cyber Security and the impact of cyber attacks during the Russia-Ukraine invasion. Please note that due to the complexity and evolving nature of the situation, the details and specific events mentioned may be subject to change.

5. CONCLUSION

The sophistication of technology today undeniably provides opportunities for individuals to engage in criminal activities, resulting in harm to society, commonly known as Cyber Crime. This is evident in the case of Ukraine, where the ongoing conflict between Russia and Ukraine has caused significant losses for both parties. The battle is now taking place in the digital realm, where digitalization has become a part of daily life and has enabled Russia to easily attack Ukraine not only through military invasion but also through the use of technology. One prevalent and highly damaging cybercrime is ransomware, a type of malicious software or malware that threatens victims by destroying or blocking access to critical data or systems until a ransom is paid. Historically, ransomware primarily targeted individuals, but recently, human-delivered ransomware targeting organizations has become increasingly widespread and challenging to prevent and address.

In the recent Russia-Ukraine conflict, Western leaders have firmly stated that they will not send military forces to engage in the war in Ukraine. However, in the digital realm, Western government, military, and commercial actors are directly involved in cyberattacks against Russia and take responsibility for defending Ukraine's networks and data. The strategic context shows that despite Ukraine's experiences in defending against Russian cyber attacks and its highly capable experts in protecting critical targets, it will ultimately be unable to prevent significant damage and exploitation of Ukraine's digital networks and data.

The conflict between Russia and Ukraine has brought about various impacts not only on economic, political, and intergovernmental cooperation aspects but specifically on Cyber Security. Russian cyber attacks continued until February 24, 2022, concurrent with Russia's military invasion of Ukraine. These attacks targeted Ukraine's communication systems and satellites one hour before the invasion. Apart from only a few countries willing to provide assistance to Ukraine, the limited capabilities also contribute to the difficulty in containing cyber attacks due to Russia's expertise. Moreover, Russia denies the cyber attacks they have conducted, and cyber attacks often prove difficult to predict in terms of their timing. However, Ukraine has strategies in place that encompass securing critical services such as energy networks, etc. These strategies aim to enhance security and focus on development to respond to major cyber attacks, as well as collaborate with global partners to ensure cybersecurity and stability in the digital realm. While the specific mention of Ukraine's cybersecurity is not provided, information security, considered vital, is mentioned in terms of protection and is assumed to encompass cybersecurity. Threats related to information security covered by the mentioned laws include the disclosure of state secrets or other prohibited information crucial for protecting national interests, computer crimes, and computer-based terrorism, as well as the dissemination of false information.

REFERENCE

[1] Microsoft, 2020. "What is Ransomware?". https://www.microsoft.com/id-id/security/business/security-101/what-is-ransomware

[2] Fedor Octav, (2022). "93 Must-Know Ransomware Statistics". https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=Cj0KCQjwyLGjBhDKARIsAFRNgW-Ku6qN-jusHmC4dOC8RFw6wwll4tboKELVY-i4Xnzvt DoT82J2Nw8aAgRfEALw_wcB

[3] Widi Shilvina, (2023). "Pengguna internet di Dunia Mencapai 5,3 Miliar pada 2022" https://dataindonesia.id/digital/detail/jumlah-pengguna-internet-di-dunia-mencapai-53-miliar-pada-2022

[4] Yudi Herdiana, Zen Munawar, Novianti Indah Putri, (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. Jurnal ICT : Information Communication & Technology Vol. 21, No.1, Juli 2021.

[5] Nick Beecroft, (2022). "Evaluating The International Support To Ukrainian Cyber Defence" https://carnegieendowment-org.translate.goog/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc

[6] Sonny Sudiar (2018). Pendekatan Keamanan Manusia dalam Studi Perbatasan Negara. Jurnal Hubungan Internasional vol. 7 no. 2.

[7] Hardianto Djanggih, Nurul Qamar (2018).Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). Pandecta Jurnal Penelitian Ilmu Hukum vol. 12 no. 1.

[8] Paul R. Kolbe, Maria R. Morrow, and Lauren Zabierek (2022). The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict. Harvard Business Review https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict

[9] SULSELPROV-CSIRT, 2022. https://csirt.sulselprov.go.id/portal/berita/17. antaranews.com. "Mewaspadai dampak serangan siber perang Rusia-Ukraina." https://www.antaranews.com/berita/2737877/mewaspadai-dampak-serangan-siber-perang-rusia-ukraina

[10] Bateman, Jon, 2023. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications." Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657

[11] Kumparan, 2023.. "Peran NATO dalam Peristiwa Cyber Attack Rusia di Kawasan Eropa". https://kumparan.com/virmindrakayla/peran-nato-dalam-peristiwa-cyber-attack-rusia-di-kawasan-eropa-1z6fPqsJz41

[12] POLITICO, 2023. "Ukraine Calls for 'Cyber United Nations' amid Russian Attacks," https://www.politico.com/news/2023/01/15/ukraine-cyber-united-nations-russia-00077955

[13] "The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments" https://link-springer-com.translate.goog/article/10.1007/s41125-017-0020-x?error=cookies_not_supported&code=32c23acc-d827-4065-b3c0-80f0c24d33a3&_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc