

## “Independent” Ukrainian “Kill List” Actually Run By Kiev, Backed by Washington

### Description

Late last year, my name was added to a blacklist published online by the Ukraine Center for Countering Disinformation. I joined over ninety others deemed to be “speakers who promote narratives consonant with Russian propaganda.”

These included Manuel Pineda and Clare Daly, both leftist Members of the European Parliament (MEP); Also counted are people on the right, such as Doug Bandow of the Cato Institute, neocon and former IDF officer Edward Luttwak, a slew of rightist MEPs; Ex CIA officer, Ray McGovern; former military and intelligence figures such as Scott Ritter and Douglas McGregor, as well as academics such as John Mearsheimer and Jeffrey Sachs. Journalists on the list included Glenn Greenwald, Tucker Carlson and Eva Bartlett, Roger Waters from Pink Floyd, and even actor Steven Seagal.

????? ?????? ????????? = David Miller, Journalist - in Ukrainian  
????? ??????, ????????? = David Miller, Journalist – in Ukrainian

What was my crime? It said my “pro-Russian narrative” was claiming that “NATO’s proxy war with Russia is taking place in Ukraine”. Of course, a NATO proxy war is exactly what is happening there, as this article will only further confirm.

The listing helpfully provided a link with the evidence, an article I wrote for *Mayadeen English* called “How disinformation works: Western intelligence agencies global war on the left.” It contained a single, 176-word paragraph on Ukraine titled “‘Russian Disinformation’ or Ukrainian lies?” It recounted several examples of Ukrainian misinformation and concluded that “Anyone who mentions any particular truth is derided for echoing Putin’s ‘talking points’.” In the event I was actually denounced as an “information terrorist” who might be guilty of “war crimes.”

Being added to the blacklist concentrates the mind wonderfully on the forces ranged against the possibility of truth and justice in the crisis-ridden West. When I was first accused, over a decade ago now, of antisemitism, my response was to intensify my research and writing activities on the organizations involved in defaming me. Since then I have produced a long catalog of work on the Zionist movement as well as on Western propaganda activities. Of course, the defamatory attacks

encourage an atmosphere where social media threats can be made. But the issue of Nazism in Ukraine will be seen in retrospect as a defining issue of our era and it is important to remember that the reason I and many others are threatened by the Ukraine government and their NATO backers is because we in turn threaten to expose them for what they are: Nazi collaborators.

## The NATO-backed kill list

But what is the Center for Countering Disinformation? It is an official governmental body created in late March 2021, along with a similar organization, the Center for Strategic Communication, by President Zelensky himself. But are they related to other blacklisting websites like Myrotvorets (“Peacemaker”), widely seen as a “kill list”? Peeling back the layers of cover and deception enables us to trace the origins of the kill list, which is still being hosted in Ukraine.

As it turns out, the covert “kill list” website is a product of the Ukraine regime, effectively funded by the CIA (amongst others) and is hosted by NATO. One extraordinary thing is that many American citizens, including ex-military and intelligence operatives, are included, as well as a significant number of citizens of NATO member countries. Perhaps the most remarkable element is that NATO has hosted the site (and a collection of affiliated websites) on its servers in Brussels. At the same time as NATO think tank the Atlantic Council boasts that Henry Kissinger is on its Board of Directors, NATO also hosts a kill list website on which Kissinger appears.

[Henry Kissinger is on the kill list.](#)

Image not found or type unknown

Henry Kissinger is on the kill list

Don't believe me? Let's take a look.

Let's start with the kill list website itself, Myrotvorets. Today it is located at Myrotvorets.center, but it was originally at psb4ukr.org. That domain was first registered on 14 August 2014, some six months after the U.S.-backed Maidan coup that overthrew the democratically elected government of Viktor Yanukovich. Other similar domain names were later logged for the group, including the following (date of first registration in brackets):

- [Psb-news.org](#) (3 April 2015)
- [Psb4ukr.ninja](#) (19 April 2015)
- [Psb4ukr.net](#) (7 May 2015)
- [Psb4ukr.xyz](#) (8 November 2015)
- [Report2psb.online](#) (19 August 2017)

These were used either as mirror sites, as digest news from the site, or, in the case of the last one, a

form for reporting suspects. The Myrotvorets.center domain name was first registered on 7 November 2015 and the site was live by February 2016.

Three people are associated with these domains and they provide valuable clues to who and what was involved in the kill list site. They are:

- **Victor/Viktor Garbar** is a longstanding Maidan activist and co-ordinator of the Maidan Monitoring Information Center. He was the first registrant of a Myrotvorets domain name in August 2014 – psb4ukr.org. He had previously owned the domain of Maidan Monitoring from 2001 – maidanua.org (now located at maidan.org.ua). The group has been in existence since before the so called “Orange Revolution” in 2004. It was, of course, funded by the National Endowment for Democracy the foundation [known as](#) the “CIA sidekick” and the International Renaissance Fund, the Ukraine branch of the Open Society Foundation run by George Soros.

- **Vladimir/Volodymyr Kolesnikov** is a webmaster and developer. He has never given any public indication that he is affiliated with Myrotvorets. Among the links to the kill list are that a domain he owns ([free-sevastopol.com](#)) now redirects to Myrotvorets.center and he registered [psb-news.org](#) which is devoted to Myrotvorets news.

- **Oksana/Oxana Tinko** was the first to register the domain Myrotvorets.center and she also registered several others related to the kill list project such as Psb4ukr.ninja, Psb4ukr.net and Psbr4ukr.xyz

## Operation Butterfly – the prototype kill list

Tinko is also the registrant of a series of domains that appear to be components of the Myrotvorets project and one that appears to have been a prototype. It is particularly stark in its intention to use the website to kill traitors or “terrorists”. The domain Metelyk.org was [first claimed](#) on 21 July 2014, three weeks before the first Myrotvorets domain. Metelyk is the Ukrainian word for Butterfly. The website titled Operation Butterfly was online by late August 2014, the first holdings in the Internet Archive are from the 27th of that month.

[Operation Butterfly website](#)

Image not found or type unknown

Operation Butterfly website

Website FAQs [make it clear](#) that it considers calling “for separatism or changes in the constitutional system” a crime. The site states the necessity “to take appropriate measures in the event that the court, the police, the SBU, or the prosecutor’s office is trying to release terrorists and their accomplices from the arms of the law”. The FAQs are even more explicit on what is meant by “appropriate measures.”

*Q: Last question: why “Butterfly”?*

*A: The site’s logo features a butterfly known as the “deadhead hawk”. In Latin, it has the name Acherontia atropos, where the first word comes from the name of the river in the realm of the dead in ancient Greek mythology, and the second is the name of the goddess of fate, who cuts the thread of*

*human life. This symbolism should remind the enemies of Ukraine that their fate currently hangs on a very thin thread, and we will do everything to break this thread.*

In late 2014 another associated site – Operativ.info – was in action calling for information about saboteurs and terrorists and [threatening](#) that if disinformation was detected, they would “regard these actions as assistance to terrorists and take measures against disinformers”. Revealingly the Operativ.info site [was](#) labeled as a project of InformNapalm at this stage.

Myrotvorets lists thousands of “saboteurs”, “separatists”, “terrorists” and “traitors”. Sometimes, it has crossed out their photographs once they had been killed, with the label “liquidated”. This, for instance, [happened](#) after the murder of Daria Dugina in Moscow in August 2022. Today the Myrotvorets site houses links to two other domains which appear to be integral parts of the operation. One – [ordilo.org](#) – is titled “STORAGE OF INFORMATION ABOUT CRIMES AGAINST UKRAINE”. The other – identigraf.center – allows various categories of users to submit images of individuals for facial recognition scanning. Tinko [registered](#) both domains.

## The NATO connection

Kolesnikov and Tinko were successive registrants on [Natocdn.work](#) (from March 11, 2015). Tinko registered a follow on domain [Natocdn.net](#) (28 January 2019). These obscure-sounding web addresses were used to host the files needed for the Myrotvorets site as can be seen by examining the “page source”(right-click in Chrome and [select](#) “View page source”) on the site including in versions [held in the Internet Archive](#). The first domain name (.work) was previously used to host both the original and succeeding Myrotvorets web sites. Thus it is in the page source on psb4ukr.org on [15 December 2015](#) just before the launch of the myrotvorets.center website, and is in the latter page source when it was first captured in the internet archive on [25 February 2016](#). The archive also shows that the latter domain was later [hosted via](#) Natocdn.net.

The letters CDN perhaps refer to a Content Delivery Network, a device to speed up the delivery of web pages when they are searched from an otherwise remote location, such as the California based name servers also used by the site. In fact, the Natocdn.net domain is [hosted](#) at none other than the official website NATO.int, based at its headquarters in Brussels.

---

[Source](#)

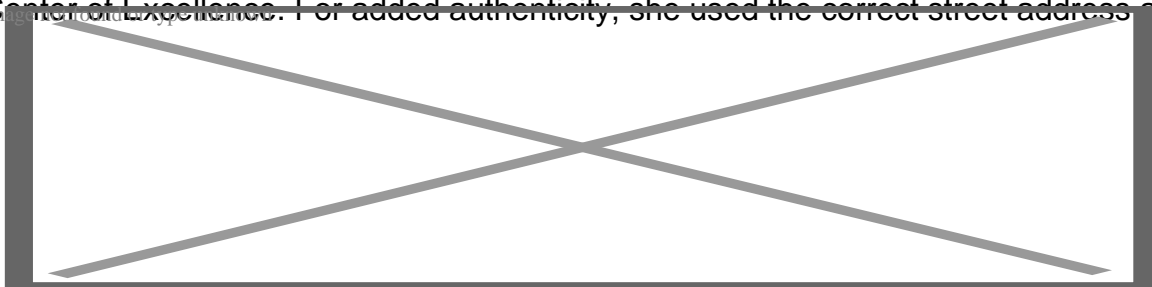
Image not found or type unknown  
[Source](#)

Back on 17 April 2015, several interested people had [also tracked](#) the original web address (psb4ukr.org) directly to nato.int without the intermediary “CDN” domain suggesting that Myrotvorets had been hosted there from near the beginning. Other IP history records show that the [Operation Butterfly domain](#) discussed above was also hosted on psb4ukr.nato.int, [as were](#) two other sites:

- [zoperativ.info](#) which we noted above was part of the Myrotvorets operation;
- [informnapalm.org](#)

The latter was [described](#) “as anti-Russian propaganda site.” While this is certainly true, that designation seriously underestimates the importance of that domain in this story, as we shall see.

A day or so after this exposure in April 2015, Oxsana Tinko [registered](#) a new site for the project: psb4ukr.ninja. Perhaps foolishly, perhaps in an attempt to lean into the disclosure, she gave her location as Estonia and her company as NATO CCDCOE – the NATO Cooperative Cyber Defense Center of Excellence. For added authenticity, she used the correct street address and phone number.



The NATO center

quickly put out a statement [denying any link](#), reading:

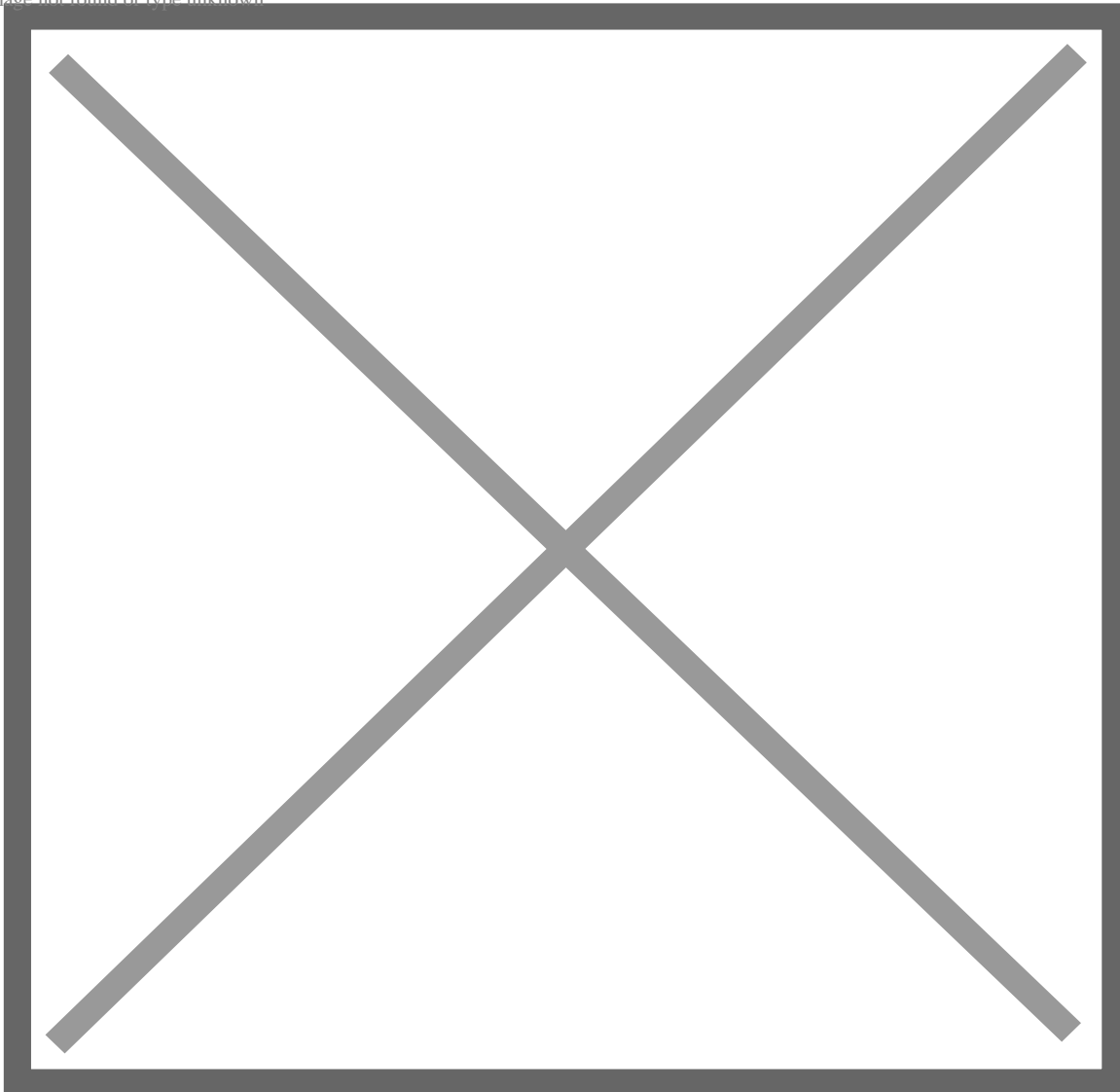
In fact, the Centre of Excellence has absolutely no connection with the site mentioned...

Oxana Tinko ... has no affiliation whatsoever with the NATO Cooperative Cyber Defence Centre of Excellence... [She] appear[s] to have hijacked the Centre's public information and we are taking steps to get the false information removed.”

It is also noteworthy, however, that a Ukraine Ministry of Defense psyops Powerpoint from 2015, leaked in the same month of that year (April), [refers](#) to the NATO cyber center as one of seven Western groups with which it had “cooperation”.

Nevertheless, the link to the NATO servers remained in the page source of the Myrotvorets websites. It was not until the NATO connection became an issue again in late August 2022 that anything was done about this. This was after Henry Kissinger had been added to the site in May. Then on August 24, independent journalist Eva Bartlett (who was named on both the Myrotvorets and Center for Countering Disinformation lists) [reported that](#) the page source code for Myrotvorets included links to resources held at psb4ukr.natocdn.net. Later, on October 14, she drew attention to the fact that Elon Musk had been listed on the site briefly after he threatened not to continue supplying his Starlink system to the Ukraine military for free. Musk responded “Is this list real?” Within eight days the page source links to natocdn.net were gone.

Image not found or type unknown



More than one hundred links to natocdn.net were still there on [October 21, 2022 at 22:35](#) but were all gone by the [next morning at 09:14](#). Even after the incriminating text was removed, however, IP tracking sites show the domain natocdn.net is [still](#), at the time of writing ([Archive version](#)), mounted on servers at NATO headquarters in Brussels. In fact, many of the image files used to make up the site are still hosted at that URL including the gory front page [collage](#) of alleged dead Russian soldiers. ([Archive version](#)).

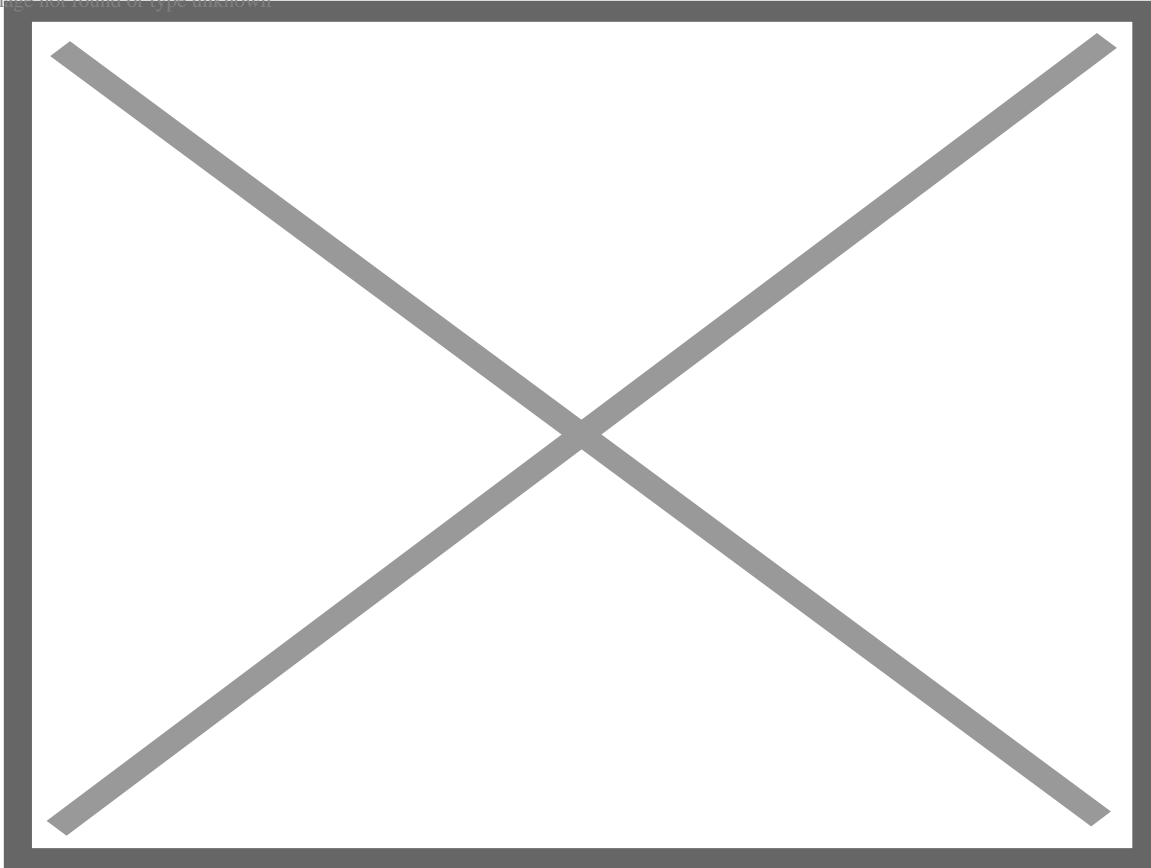
But what of Informnapalm.org – the other site which appears to have been hosted on nato.int? The evidence suggests that Myrotvorets is a project of InformNapalm.

## InformNapalm as a Ukraine Ministry of Defense “special project”

InformNapalm presents itself as a volunteer-run intelligence service. But this is a deception. A

Ukrainian Ministry of Defense PowerPoint presentation [leaked in 2015](#) refers to it as a “special project” of the ministry, along with a number of others who themselves stand in need of further investigation.

Image not found or type unknown



Corroborating information comes in the form of the identity of the person who registered the domain name informnapalm.org – the aforementioned Vladimir Kolesnikov on [March 29 2014](#), six months before the first of the kill list domains were registered. Kolesnikov is the [webmaster](#) of InformNapalm. His LinkedIn page [describes](#) his involvement with InformNapalm as beginning as a “translator” in February 2014, graduating to System Administrator in March 2014 and DevOps engineer in April 2014. Helpfully Vladimir lists another “volunteering” role from February 2014 with the Ministry of Defense of Ukraine. This role involved: “participation in information operations in the interests of the anti-terrorist operation in Donetsk and Luhansk Oblasts, and assistance in counteraction to information aggression by the Russian Federation.” Myrotvorets is, therefore, a project of InformNapalm which is, in turn, a “special project” of the Ministry of Defense.



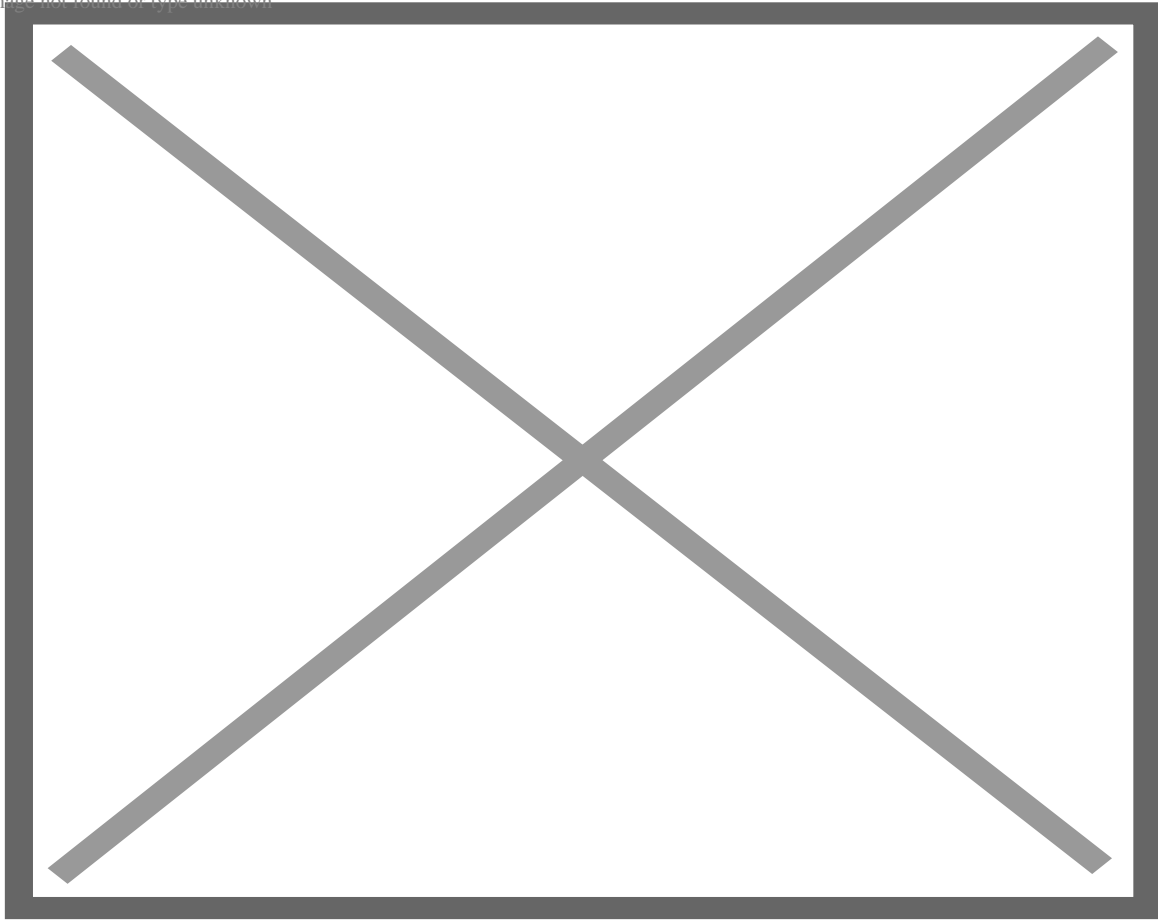
[Volodymyr Kolesnykov | LinkedIn page](#)

Image not found or type unknown

[Volodymyr Kolesnykov | LinkedIn page](#)

Other links between the two projects include that Oksana Tinko, in registering the domain Myrotverots.center, used her informnapalm.org email address. On her Facebook page she claims to have worked at InformNapalm since March 2014. This conforms to the detail in [data released](#) by the Russian hacking group Cyber-Berkut which showed that Tinko had become an admin on the Operativ.info and informnapalm.org sites on March 29 2014.

Image not found or type unknown



Oksana Tink on Facebook | [Source](#)

Tinko is fond of displaying Nazi and Banderite imagery on her social media. There is a swastika on her Github page and her Facebook profile features a background with the red and black colors of Bandera and a star of David together with a reptilian dressed as an orthodox Jew.

The journalist George Eliason who excavated much of the story of InformNapalm reports that the people involved are “mostly Pravy Sektor” (Right Sector), in other words far right supporters of Stepan Bandera. Pravy Sektor uses the red and black colors of Bandera in its flag, just as Tinko does on her Facebook profile. In late 2019 Myrotvorets proudly displayed a portrait of Bandera on its homepage to mark the Nazi collaborator’s birthday.

Image not found or type unknown



“January 1 — [Stepan Andriyovych Bandera’s birthday](#)”

In the early days of the Myrotvorets project the InformNapalm logo was prominently displayed. It was still there on May 13, 2016, but was gone by August of that year. This may have been because of its publication of the list of thousands of journalists’ names which caused significant backlash and led to a statement that “taking into account the reaction... the Center ‘Peacemaker’ made a difficult decision to close the site.” The site did not shutter, however. By 2017, Myrotvorets continued to boast of its links with InformNapalm, stating:

Volunteers of the Ukrainian Cyber Alliance (UCA), the intelligence community InformNapalm and the Peacemaker Center publish their research based on information contained in the mail of terrorists and Russian authorities.”

As this passage highlights, all three organizations worked closely together.

InformNapalm logo 2014 and 2023 - showing how it has tried to mellow its image.

Image not found or type unknown

InformNapalm logo 2014 and 2023 – showing how it has tried to mellow its image.

It would appear that InformNapalm is the parent or coordinating body for an evolving team of pro-Ukrainian hackers, researchers, journalists and devotees of the far right. InformNapalm claims that: “We mostly rely on open sources and widely employ different OSINT methods of information gathering. We also receive some information from insiders (HUMINT) and hacktivists.” It also claims: “InformNapalm does not participate in or encourage computer hacking activities.”

This is an admission of receipt of intelligence information (“Humint”) from Ukrainian and perhaps other intelligence services. The disavowal of participation or encouragement of hacking is undermined by their own statements, as in this one by one of the hackers:

At first we had a separate group called RUH8... Our cooperation with other hacker groups was established thanks to the InformNapalm ...where we all submitted information for processing and publication.”

RUH8 is an abbreviation for Russia Hate. InformNapalm [claimed in 2020](#) that it “is a purely volunteer endeavour which does not have any financial support from any government or donor.” This is, of course, a lie.

## Prometheus

It is a matter of public record that InformNapalm has been funded by the National Endowment for Democracy, the CIA proxy. For example, in its now-deleted list of funding for Ukraine in 2016, the NED reported that \$100,000 was given to a project of “Prometheus”. It would “conduct open-source investigations that monitor and spotlight external Russian military actions and post them on its popular and trusted website, <https://informnapalm.org>”. The Prometheus domain Prometheus.ngo was also registered by Volodymyr Kolesnykov on March 11, 2016.

Prometheus advertises two “information partners” in its operation, InformNapalm and The Ukraine Media Crisis Center. InformNapalm, created in early 2014, obviously only became a project of Prometheus after the latter was created in 2016.

The Ukraine Crisis Media Center is of course another Western-funded project. It even admits to a long list of Western State funding on its website (including USAID, Embassies of the U.S., Netherlands, Switzerland, Finland, Norway, Sweden and Germany), as well as military/intelligence funding agencies such as the NED, NATO, the U.K. based Institute for Statecraft (a military intelligence cut out), regime change enthusiasts at the Soros network of foundations and the Open Information Partnership an MI6 funded project from the U.K., in which Bellingcat and other MI6 contractors were/are involved.

An avalanche of Western cash has been showered on such organizations, all of which appear to have gone to some trouble to disguise their real origins and connections (including to each other), not to mention their affiliations to the Banderite far right.

## Back to NATO

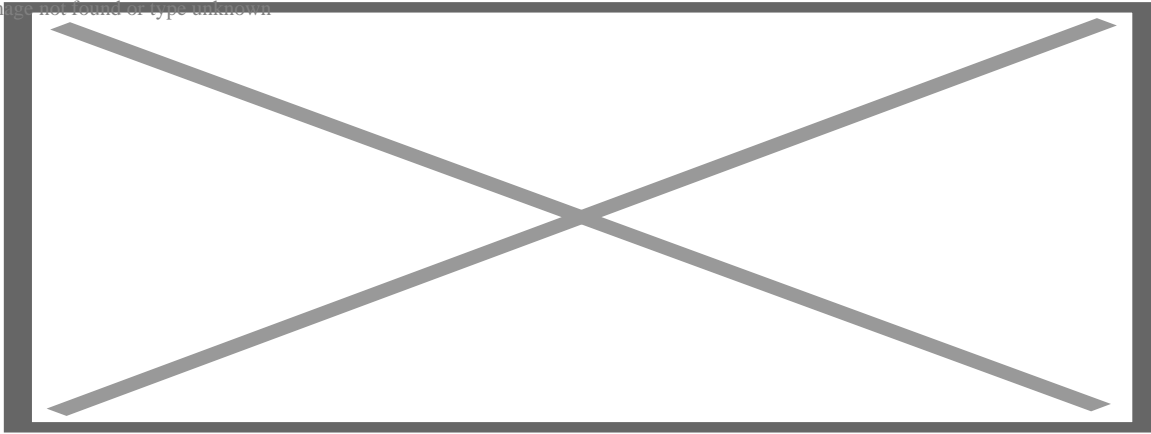
InformNapalm boasts in its list of achievements of working closely with NATO run groups such as the Atlantic Council Digital Forensic Lab and MI6/CIA cutout Bellingcat. It claimed to have identified “persons who could be involved in the shutdown of Flight MH17 ... (this information was used in the reports by our colleagues from Bellingcat team).” The organisation also claims to have conducted “exclusive analysis of SurkovLeaks – the email dump belonging to [Russian politician] Surkov’s reception office obtained by Ukrainian Cyber Alliance (the authenticity of the emails was reconfirmed by several reputable organizations, including Atlantic Council’s DFR Lab)”. The DFR Lab and Bellingcat, are not “reputable” organizations but rather are part of NATO information operations against Russia.

These boasts put both the DFR Lab and Bellingcat in the frame as collaborators with the Nazi kill list, which is itself based on the OSINT techniques pioneered by both groups. Now that we know that the “volunteers” of Mirotvorets, InformNapalm and the Ukraine Hacker Alliance are a project of the Ukrainian government with significant NATO support, the role of the DFR Labs and Bellingcat appears to be part of that support for the Nazi kill list.

In the West, these Nazi collaborators and apologists attempt to push an altogether softer narrative. Thus, we have Eliot Higgins of the Informnapalm “colleague” Bellingcat attempting what he presumably thought was a condescending denial in [tweeting](#): “Myrotvorets is a Ukrainian government kill list’ is

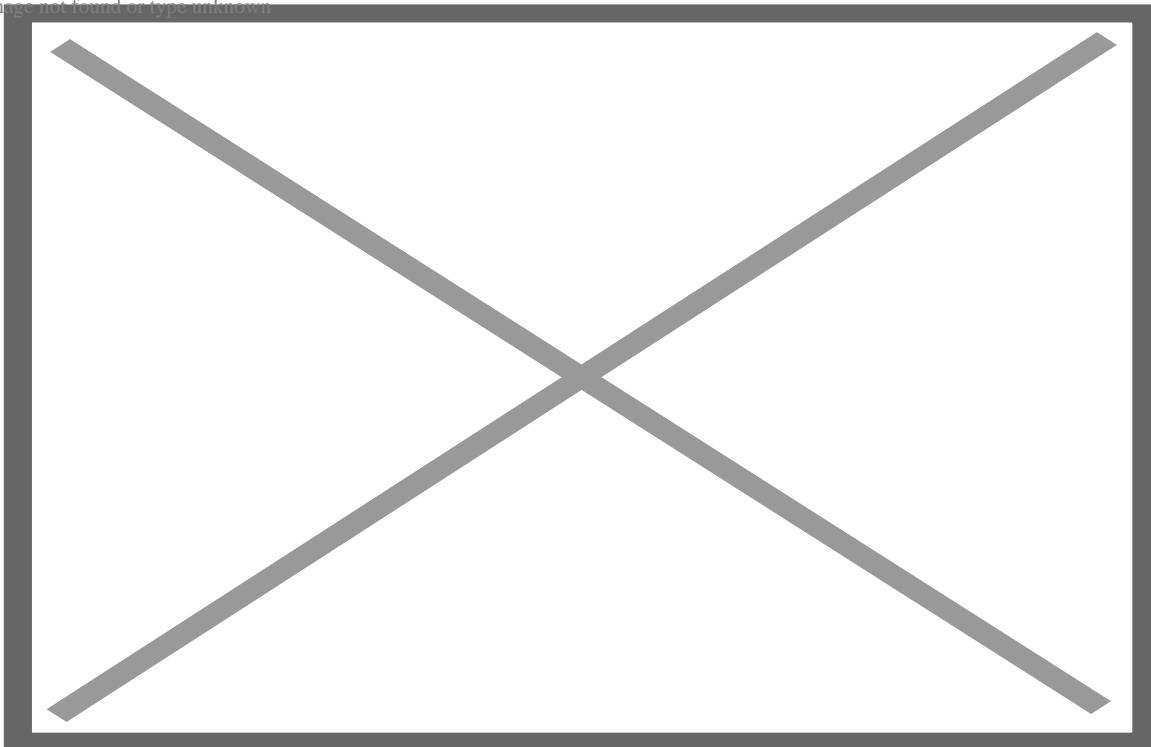
rapidly becoming the most effective way to identify the dumbest people in this website.”

Image not found or type unknown



We can even find Aric Toler, also of Bellingcat, criticizing Myrotvorets while appearing to disavow any knowledge that Bellingcat had worked with them. In response, the founder of InformNapalm (and we must assume Myrotvorets too) Roman Burko, defended the activities of the kill list as purely a question of style.

Image not found or type unknown



So, the evidence here supports the contention that NATO is fighting a proxy war in Ukraine. There is a link between the Nazi kill list and the blacklist to which I was added and that is that both are operations of the regime in Kiev. A further link is the deputy head of the regime-created Center for Strategic Communication, Mykola Balaban. He cut his teeth working on the InformNapalm/Myrotvorets operation, as was revealed in a document released by Russian hackers Cyber-Berkut in late 2015 in which he featured as an admin of both the [operativ.info](http://operativ.info) and [informnapalm.org](http://informnapalm.org) sites from November 2014.

Finally, it seems likely a key reason why the Nazi kill list remains online is that it is protected by the regime, the U.S. government and NATO.

Feature photo | Illustration by MintPress News

by David Miller

**Category**

1. Crime-Justice-Terrorism-Corruption
2. Main
3. Politics-Geopolitics-Gov.-Events

**Date Created**

05/19/2023